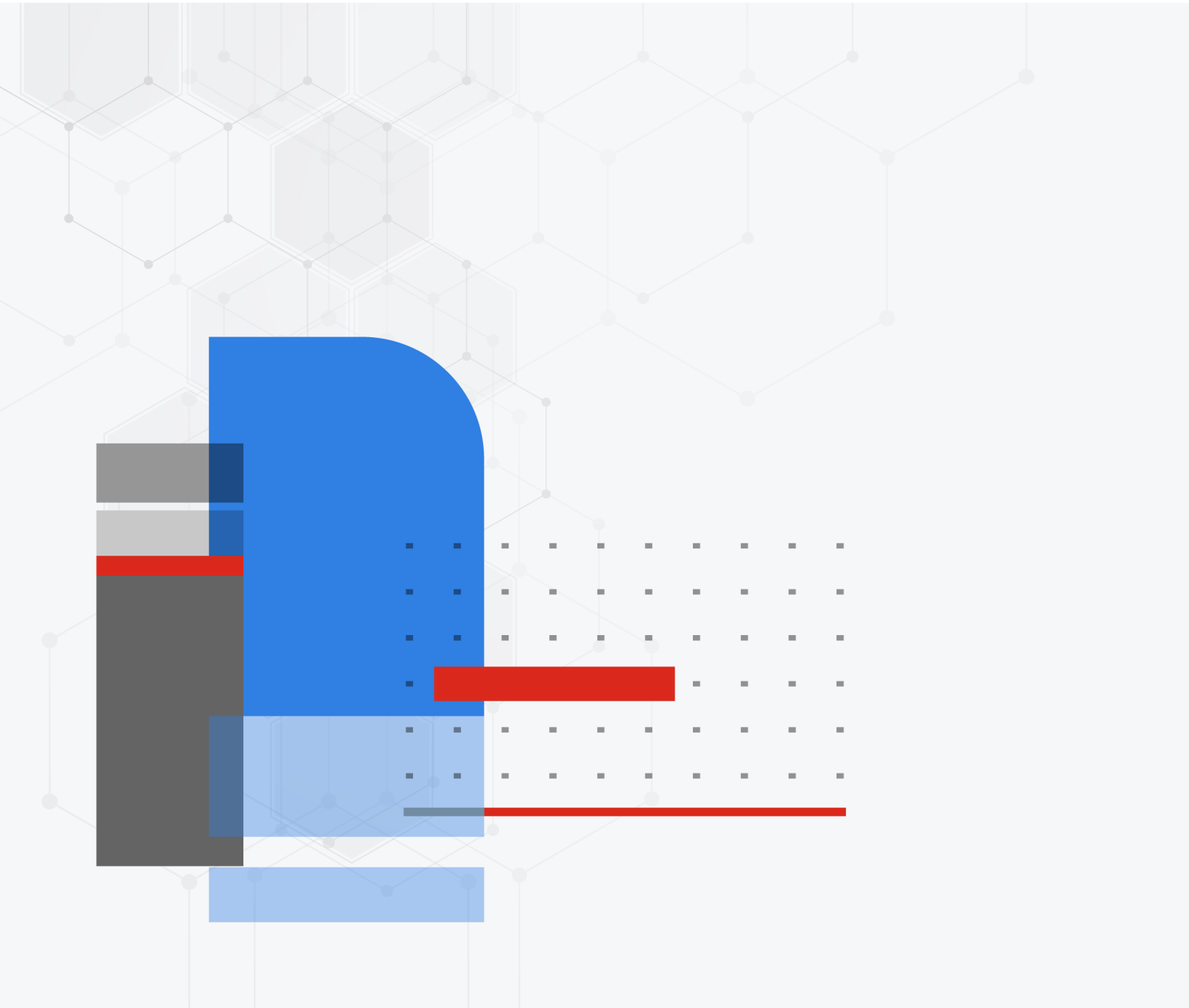




User Guide

FortiAI Ops 3.2.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

March 09, 2026

FortiAIOps 3.2.1 User Guide

83-321-1250258-20260309

TABLE OF CONTENTS

Change log	6
Overview	7
Getting Started	12
Installing FortiAI Ops	13
Initial FortiAI Ops Configuration	13
License	14
Adding FortiGate	15
Enable Log Forwarding	15
Monitoring	17
System Diagnostics	18
API Reference	19
Deploying FortiAI Ops on VM Platforms	20
Pre-installation Requirements	20
Installing FortiAI Ops on VMware ESXi	20
Installing FortiAI Ops on Hyper-V	22
Installing FortiAI Ops on KVM	30
Installing FortiAI Ops on Nutanix	32
Installing FortiAI Ops on Proxmox	36
Post-installation Tasks	38
Increasing VM Disk Space	39
Accessing FortiAI Ops	41
Upgrading FortiAI Ops	41
Deploying FortiAI Ops on Public Cloud Platforms	42
Microsoft Azure	42
Post-installation Tasks	50
Google Cloud Platform	50
Amazon Web Services (AWS)	57
Oracle Cloud Infrastructure (OCI)	62
Deploying FortiAI Ops on Hardware Platforms	66
Deploying FortiAI Ops 500G (FAO-500G)	66
Deploying FortiAI Ops 100G (FAO-100G)	68
Command Line Interface (CLI) Reference	70
Dashboard	78
Summary	78
Wireless	85
Switch	112
SD-WAN	124
Custom Dashboard	138
Managing Dashboard Widgets	142

AI Insights	146
Impacted SLA	146
Wireless	147
Switching	148
WAN	148
Impacted Devices	149
SLA Config	152
Device Health	152
Time To Connect	154
Roaming	155
Event Acknowledgement	158
FortiAI	159
Using FortiAI	160
FortiAI Data Privacy	162
FortiAI Tokens	162
FortiAI Example Tasks	163
Inventory	173
Adding and Managing FortiGates	173
Adding a FortiGate	173
Importing and Exporting FortiGates	175
Managing FortiGates	175
ADOMs	186
VDOM Support	187
Wireless	189
Access Points	189
AP	189
Radio	191
Access Points Diagnostics and Tools	192
Wireless Clients	201
Wireless Clients Diagnostics and Tools	203
Channel Summary	207
Summary	207
Events	209
Insights	209
AI-ARRP	212
Monitoring Widgets	214
Detailed Analysis and Optimization	218
Disabling AI-ARRP	222
Applications	222
Rogue APs	224
Wi-Fi Maps	225
Creating the Map Structure	226
Importing and Exporting Maps	230
Modifying the Map	232
Viewing the Map	235
Diagnostics and Tools	241

Locating Wireless Devices on the Map	242
Switch	246
FortiSwitch	246
FortiSwitch Diagnostics and Tools	246
Wired Clients	253
FortiExtenders	255
Extenders	255
SD-WAN	260
Insights	261
Forecast	265
Security Fabric	272
Physical Topology	272
Logical Topology	273
Fabric Connectors	274
Logs and Reports	275
Event Logs	275
Local Logs	281
Reports	281
Creating Reports	281
Viewing Reports	289
Scheduled Reports	289
PCI Reports	289
System	291
User Management	291
Users	291
User Groups	293
User Sessions	293
Backup and Restore	294
Settings	296
Upgrade	305
Licensing	306
FortiGuard	307
Location Services	307
Network Interface	309
Certificates	310
SAM	312
Trends	312
Completed Tests	314
Baseline Tests	315
Schedule Tests	318

Change log

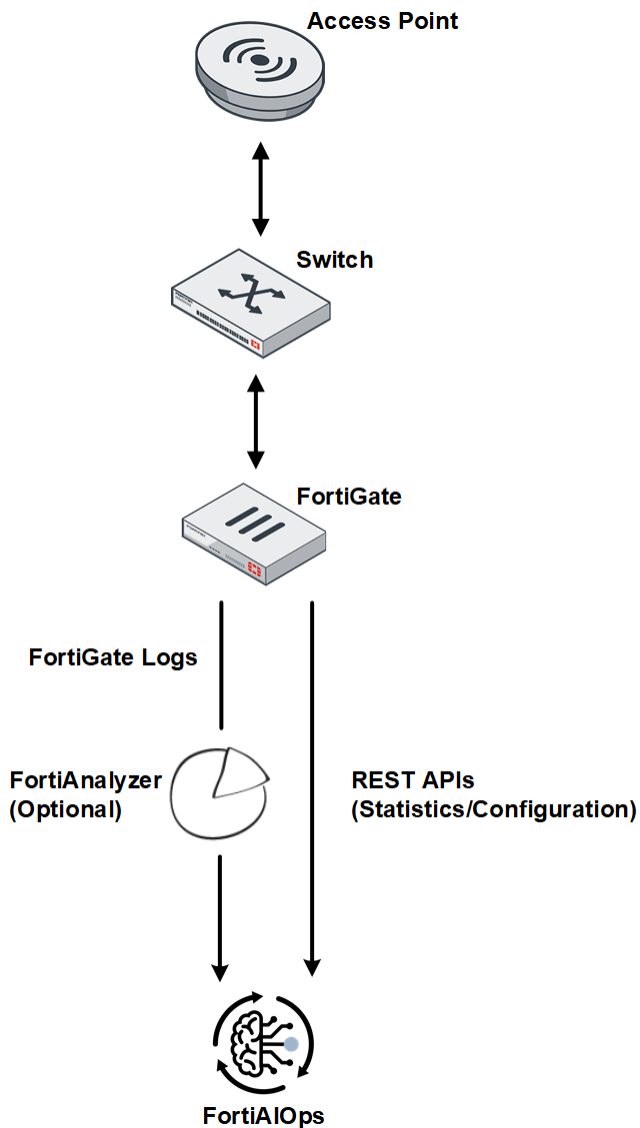
Date	Change description
2026-02-23	FortiAI Ops 3.2.1 release document.
2026-03-09	Updated Installing FortiAI Ops on Proxmox on page 36

Overview

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

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

FortiAI Ops 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 FortiAI Ops, aim at diagnosing and troubleshooting network issues by analyzing potential problems and suggesting remedial steps.



The FortiAI Ops 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.

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

- [Wireless](#)
- [Switching](#)
- [WAN](#)

Wireless

The following SLAs are monitored for wireless clients.

- [Throughput](#)
- [Coverage](#)
- [Roaming](#)
- [Time to Connect](#)
- [Connection Failure](#)
- [AP Health and Uptime](#)
- [WIDS](#)

Throughput

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

Coverage

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

Roaming

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

Time to Connect

This SLA computes the time taken by clients to connect to the network. FortiAI Ops reports those clients that take longer than certain thresholds to connect to the network. These thresholds are statically configured or FortiAI Ops 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. FortiAI Ops

displays relevant SLAs under different sections on the monitor dashboard.

WIDS

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

Switching

The switching SLAs monitor the switch health and connection status.

- [Throughput](#)
- [Network](#)
- [Switch Health and Uptime](#)
- [Switch Connection Failure](#)

Throughput

The **Throughput** SLA monitors your wired network at the system and client level, to identify potential low throughput conditions and categorizes them based on the underlying issue type, into different classifiers and sub-classifiers. Low throughput is reported based on traffic congestion due to high inbound/outbound traffic, storm conditions, low wired bandwidth conditions leading to network slowdowns, packet drops, and increased latency.

Network

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

Switch Health and Uptime

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

Switch Connection Failure

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

WAN

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

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

- [Performance](#)
- [FortiExtender Health](#)
- [Interface Health](#)

Performance

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

FortiExtender Health

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

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

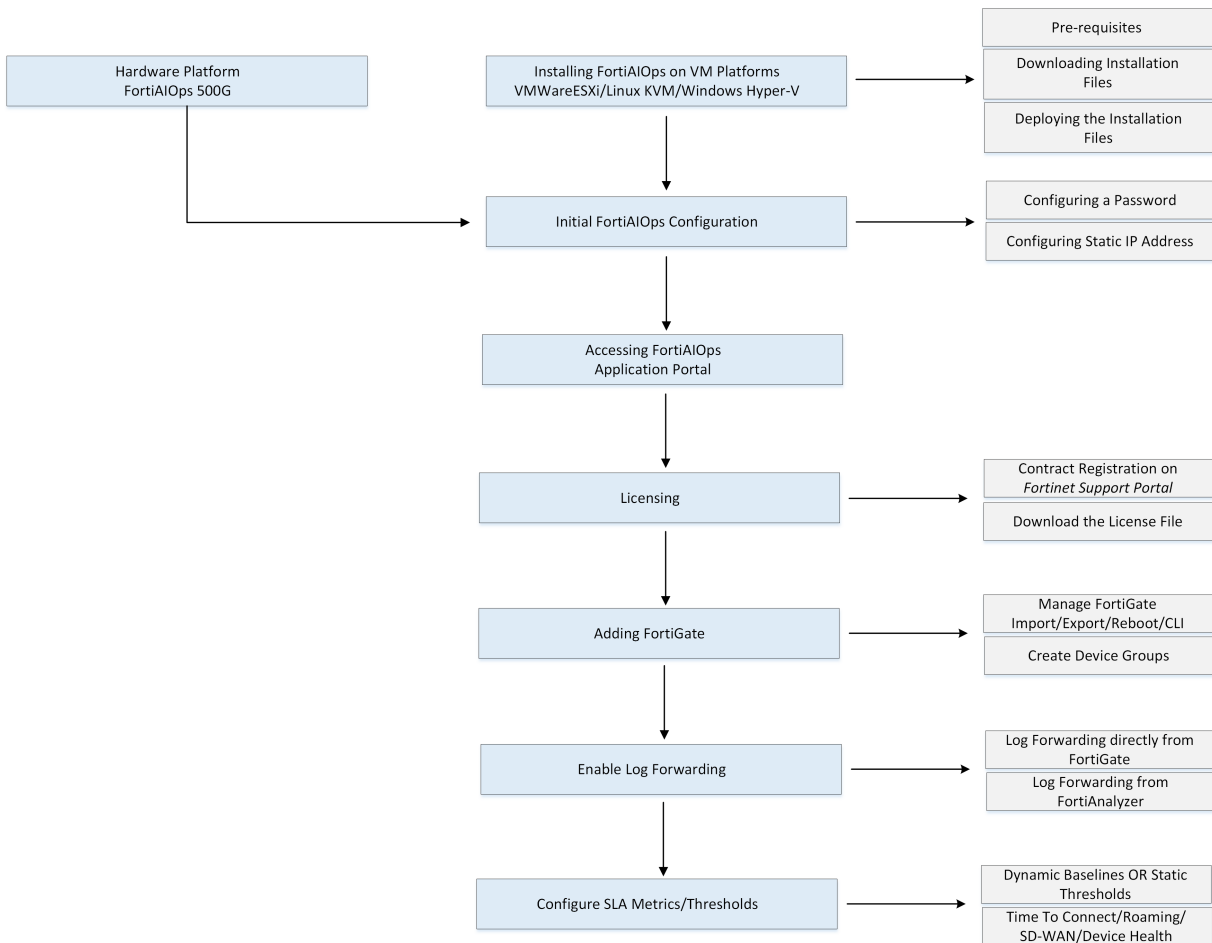
Note: FortiAIops monitors only the FortiExtender devices managed by FortiGate.

Interface Health

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

Getting Started

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



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

- [Installing FortiAI Ops](#)
- [Initial FortiAI Ops Configuration](#)
- [Accessing FortiAI Ops](#)
- [License](#)
- [Adding FortiGate](#)
- [Enable Log Forwarding](#)
- [SLA Config](#)
- [Monitoring](#)
- [API Reference](#)
- [System Diagnostics](#)

Installing FortiAI Ops

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

- **VM Platforms** - [Deploying FortiAI Ops on VM Platforms](#)
- **Public Cloud Platforms** - [Deploying FortiAI Ops on Public Cloud Platforms](#)
- **Hardware Platforms** - [Deploying FortiAI Ops on Hardware Platforms](#)

Note: The FortiAI Ops CLI and GUI users are different.

Initial FortiAI Ops Configuration

After FortiAI Ops 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.

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

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

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

License

FortiAIops offers Monitoring, AI Insights, and SD-WAN subscriptions, with licensing based on the type of devices you use. For more information, see [FortiAIops Data Sheet](#).

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

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



For FortiAIops 500G, manual license upload is not required. FortiAIops automatically synchronizes the license from *Fortinet Support*.

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

Note:

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

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

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

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

Adding FortiGate

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

You can group FortiGate controllers into **ADOMs** 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 ADOMs, see [ADOMs on page 186](#).

Enable Log Forwarding

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

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

- [Forwarding Logs from FortiGate](#)
- [Forwarding Logs from FortiAnalyzer](#)

Forwarding Logs from FortiGate

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

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

The screenshot shows the FortiGate GUI with the 'Log & Report > Log Settings' path selected. The 'Global Settings' tab is active. Under 'Log Settings', 'Event logging' is set to 'All' with a 'Customize' button. 'Local traffic logging' is also set to 'All' with a 'Customize' button. Below this, four toggle switches are shown: 'Log allowed traffic' (off), 'Log denied unicast traffic' (off), 'Log denied broadcast traffic' (off), and 'Log local out traffic' (on). 'Syslog logging' is set to 'Enable' (indicated by a green checkmark) with a 'Disable' button (indicated by a red X). The 'IP address/FQDN' field contains '10.34.207.5'. A 'GUI Preferences' section at the bottom shows 'Resolve hostnames' and 'Resolve unknown applications' both set to 'on' (green toggle).

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

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

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

For more information, see [FortiGate Administration Guide](#).

Forwarding Logs from FortiAnalyzer

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

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

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

Logging Settings

FortiAnalyzer Cloud Logging

Status ☒ Enabled ☐ Disabled

Server 10.10.10.102

Connection status ☒ Connected

Upload option

Allow access to FortiGate REST API ☒

Verify FortiAnalyzer certificate ☒ FAZ-10.10.10.102 81

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

Create New Log Forwarding

Name * FortiAIOPS_log

Status ☒

Remote Server Type Syslog

Server FQDN/IP * 3.10.10.4

Server Port 514

Reliable Connection ☐

Device Filters ☒ All ADOMs + All Devices

Operator	ADOM	Device	Action
Include	root	FG-10.10.10.102	x +

Log Filters ☐

Enable Exclusions ☐

Enable Masking ☐

Note:

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

Monitoring

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



FortiAIOPS retains user specific table configurations across sessions. Table customizations such as column visibility (adding/removing), column ordering, sorting, and filtering are automatically saved for each user and persist even after logging out, disconnecting, upgrading, and restoring.

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.
FortiExtenders	The FortiExtenders section offers details regarding the FortiExtenders, FortiExtender SSIDs, profiles, and data plans.
SD-WAN	The SD-WAN section provides comprehensive insights and forecasts on monitored SD-WAN interfaces and their associated health checks.
Security Fabric	The security fabric page represents the topology, that illustrates the logical placement of the wireless service and the physical placement of hardware devices.
Logs and Reports	The Logs section offers both detailed event logs and local logs. Logs for specific event types like WiFi Events, FortiSwitch Events, and SD-WAN Events are available. You can also generate comprehensive FortiAIOPS reports here.
System	The system section includes several pages that offer valuable insights into various aspects of system management, such as users, user groups, backup and restore, settings, licensing, location services, and certificates.
SAM	The service assurance section provides an overview of the diagnostic and trouble-prevention capability of FortiAIOPS.

System Diagnostics

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

Diagnostics

Choose content for diagnostics

☒ System Diagnostics

☒ Application Diagnostics

☒ FortiAI Ops Logs

Create File

 Download Latest File

API Reference

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

Deploying FortiAI Ops on VM Platforms

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

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

Pre-installation Requirements

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

Supported Environments

Supported environments include:

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

Hardware Requirements

The following table lists the minimum hardware requirements for deploying FortiAI Ops.

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

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

Installing FortiAI Ops on VMware ESXi

Perform the following steps to deploy FortiAI Ops.

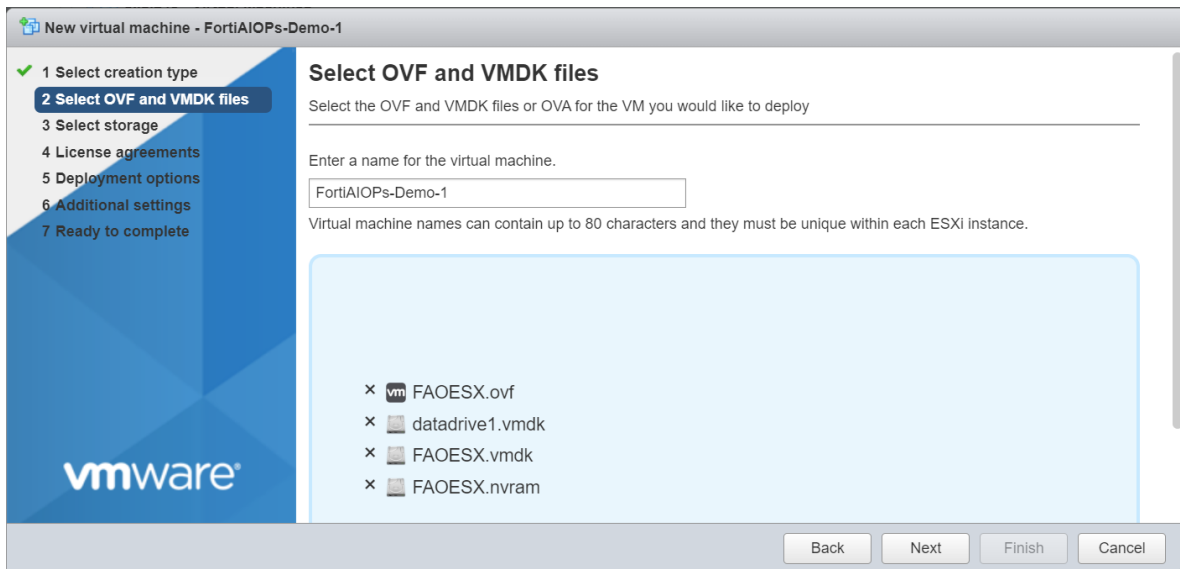
1. Download the installation file from [Fortinet Support](#) portal and unzip the file (*FAO_VM64-vx.x.x-devbuildxxx-FORTINET.out.ovf.zip*). This folder contains 4 installation files.

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

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



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



6. Select your preferred datastore to store the virtual machine files in the **Select storage** page.
7. Accept the end user license agreement.
8. In the **Deployment options** page:
 - a. Select you preferred VM network
 - b. Select your preferred disk provisioning method. Thin disk provisioning method is recommended.
 - c. Ensure **Power on automatically** option is selected

Note: To modify configurations, it is necessary to edit the VM configuration while the VM is in a powered off state, and then start the VM.

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

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 Ready to complete

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.

Back Next Finish Cancel

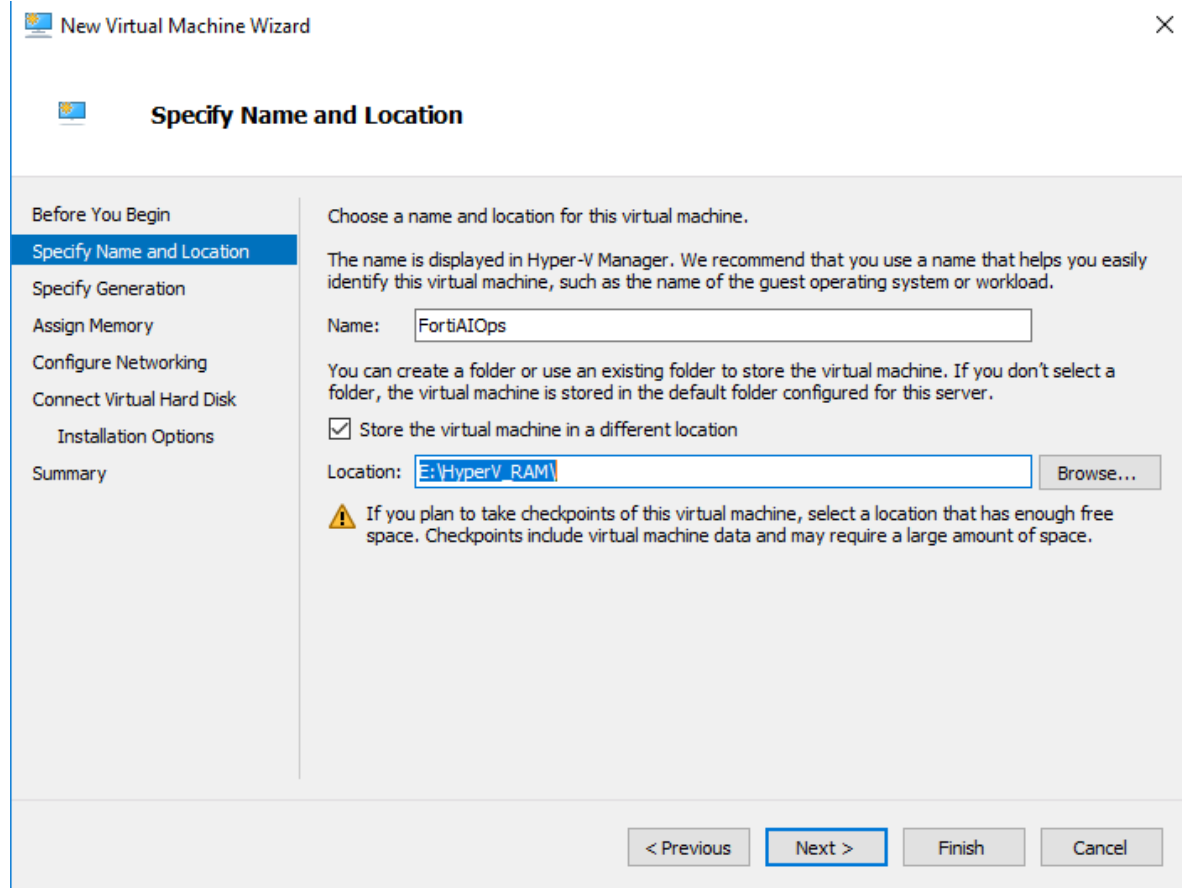
10. You can monitor the progress of the deployment in the **Recent Tasks** pane. When the installation is complete, the virtual machine will be listed in the **Inventory** pane.
11. Perform [post-installation](#) tasks.

Installing FortiAIOPS on Hyper-V

Perform the following steps to deploy FortiAIOPS.

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

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



The screenshot shows the 'New Virtual Machine Wizard' window with the 'Specify Name and Location' step selected in the left-hand navigation pane. The main area contains instructions and input fields for naming and locating the virtual machine.

New Virtual Machine Wizard [Close]

Specify Name and Location

Before You Begin

- Specify Name and Location
- Specify Generation
- Assign Memory
- Configure Networking
- Connect Virtual Hard Disk
- Installation Options
- Summary

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:

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.

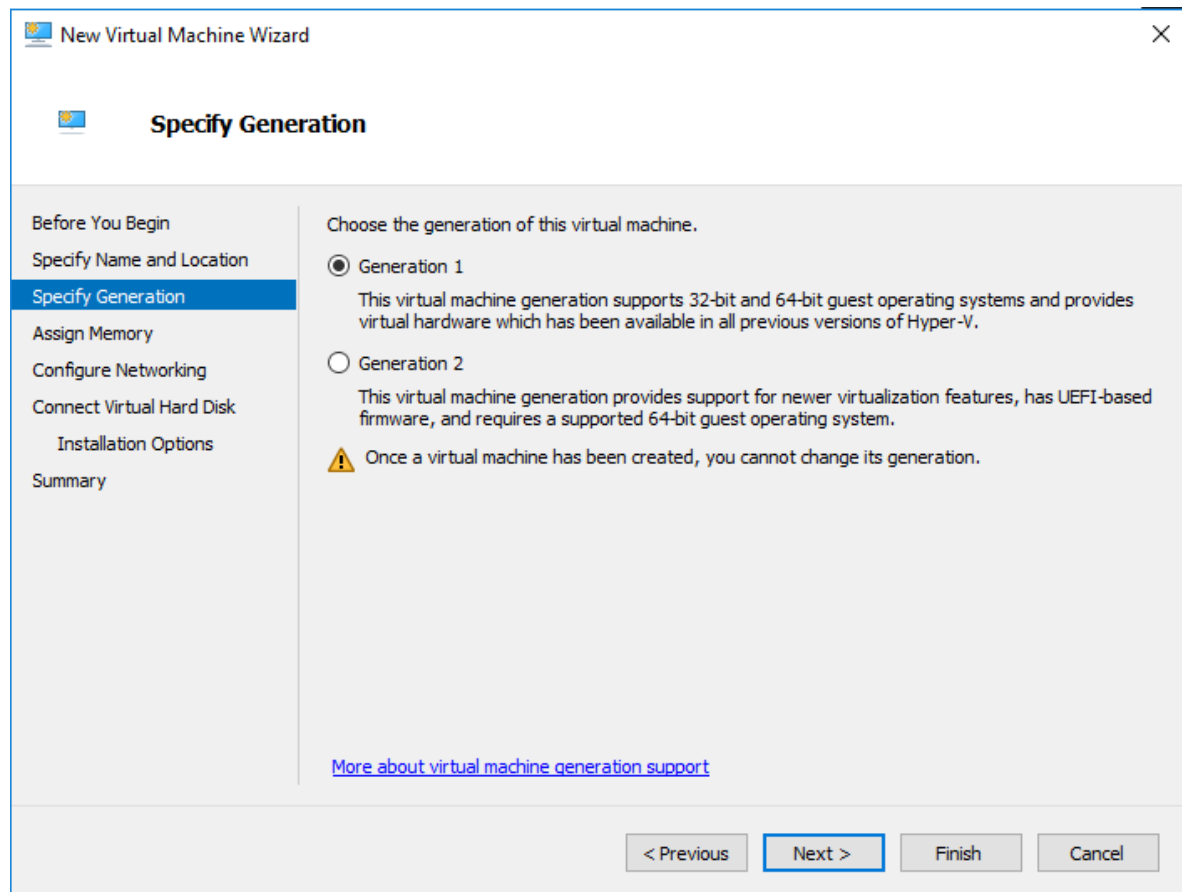
☒ Store the virtual machine in a different location

Location:

 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.

< Previous **Next >** Finish Cancel

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



6. Specify the memory that needs to be allocated. Click **Next**. See [Pre-installation Requirements](#).

The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Assign Memory' step. The window has a title bar with a close button. On the left is a navigation pane with the following steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation', 'Assign Memory' (which is highlighted with a blue bar), 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area of the wizard contains the following text: '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.' Below this text is a label 'Startup memory:' followed by a text box containing '32768' and the unit 'MB'. There is an unchecked checkbox labeled 'Use Dynamic Memory for this virtual machine.' Below the checkbox is an information icon (a blue circle with a white 'i') followed by the text: '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.' At the bottom right of the window are four buttons: '< Previous', 'Next >' (which is highlighted with a blue border), 'Finish', and 'Cancel'.

New Virtual Machine Wizard

Assign Memory

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

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.

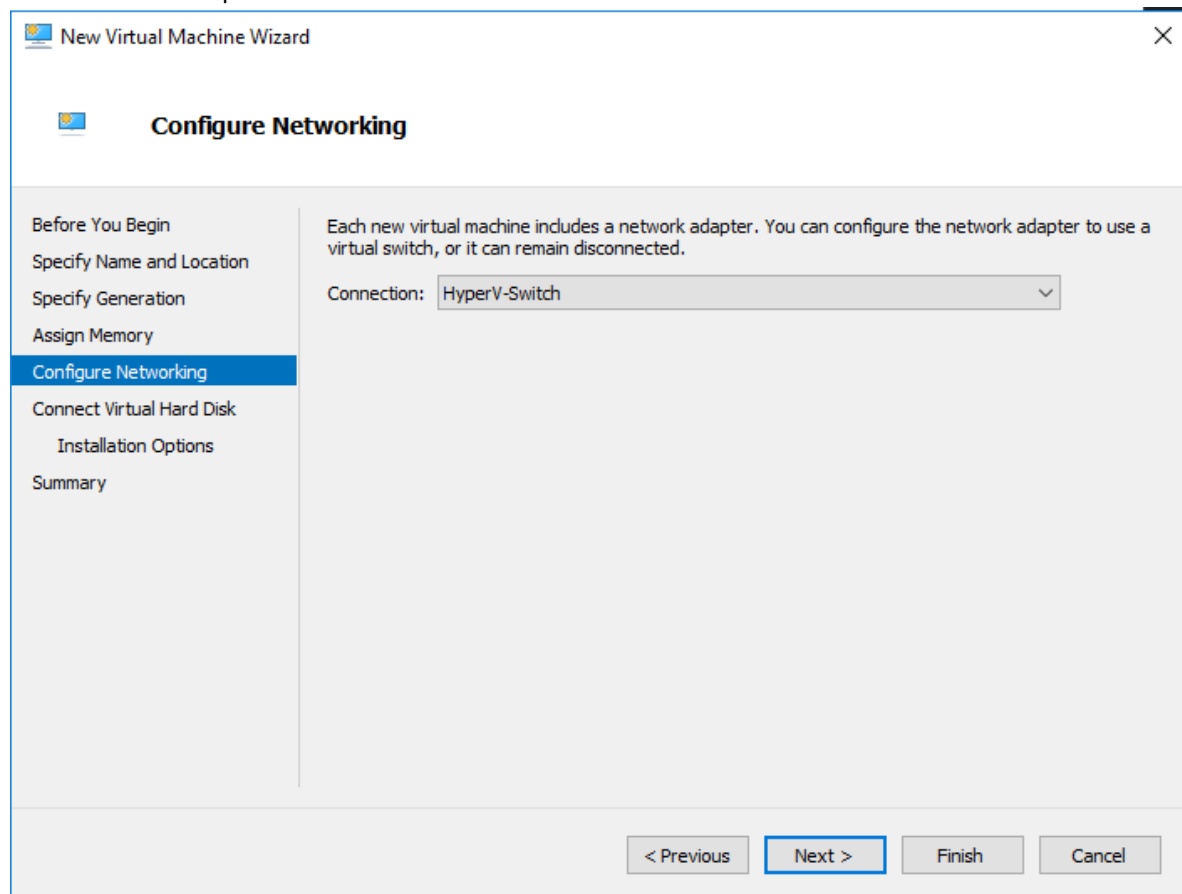
Startup memory: MB

☐ Use Dynamic Memory for this virtual machine.

i 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.

< Previous **Next >** Finish Cancel

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



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

New Virtual Machine Wizard ✕

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

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:
Location:
Size: GB (Maximum: 64 TB)

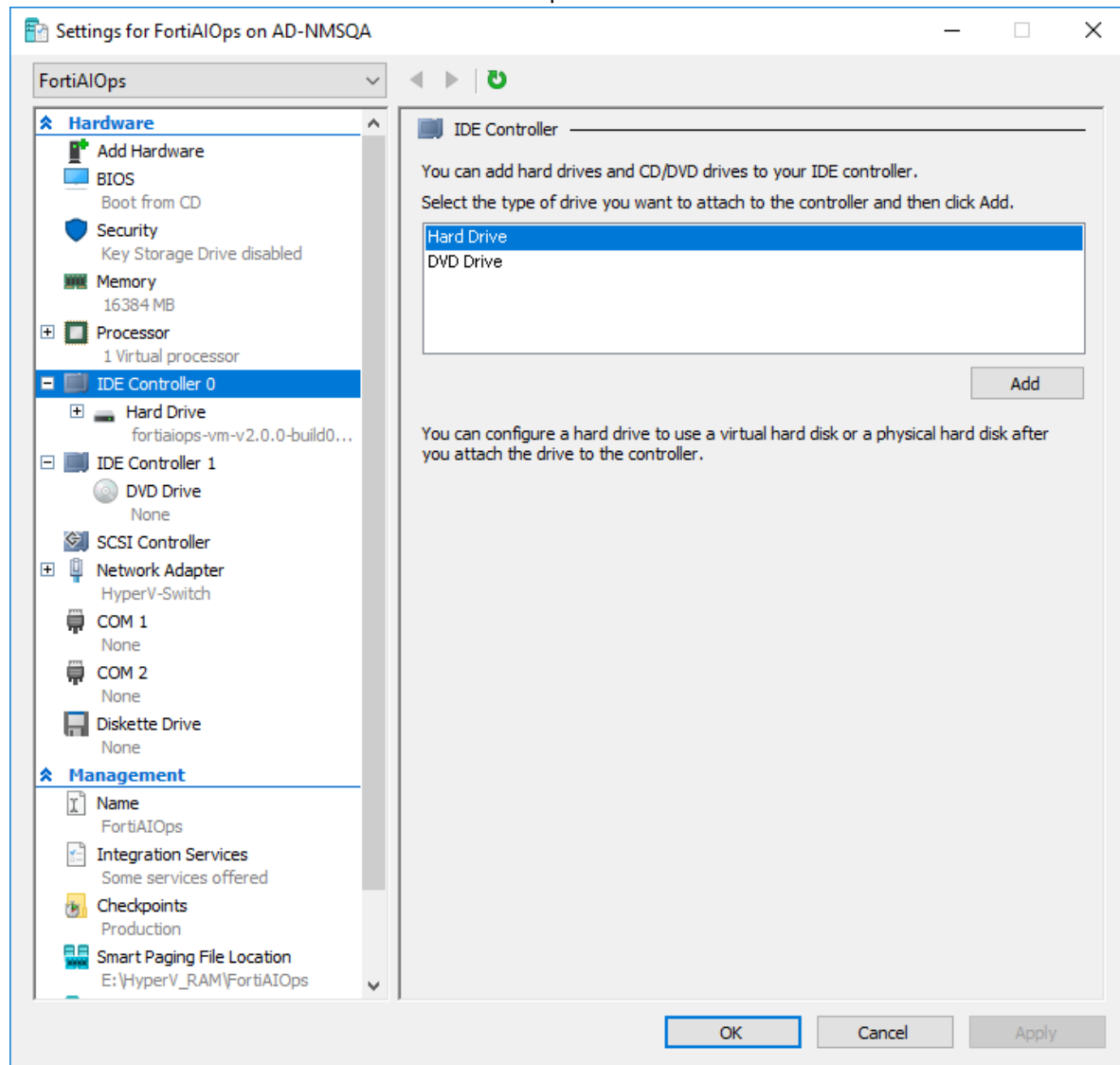
☒ Use an existing virtual hard disk
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location:

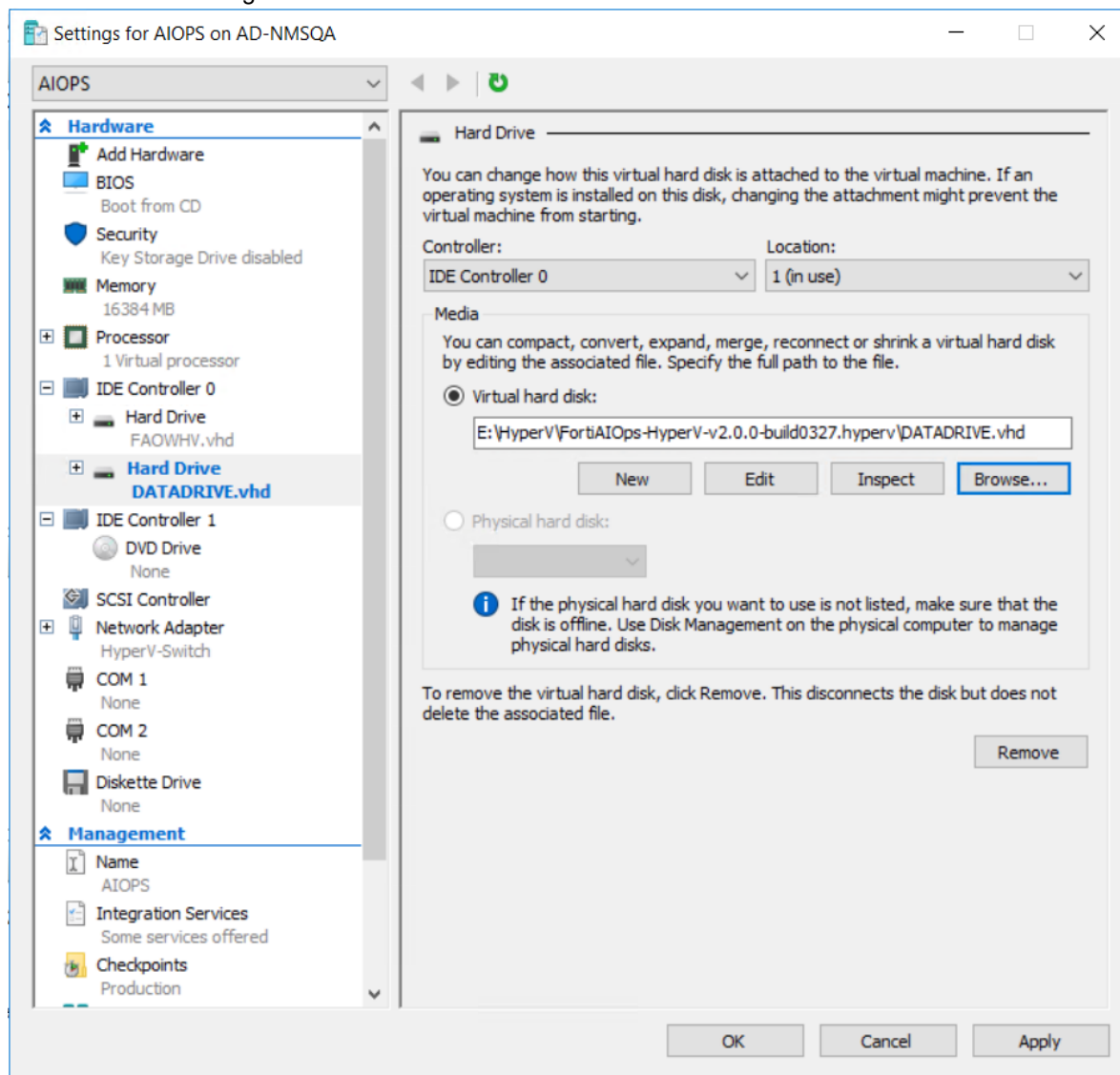
☐ Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

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

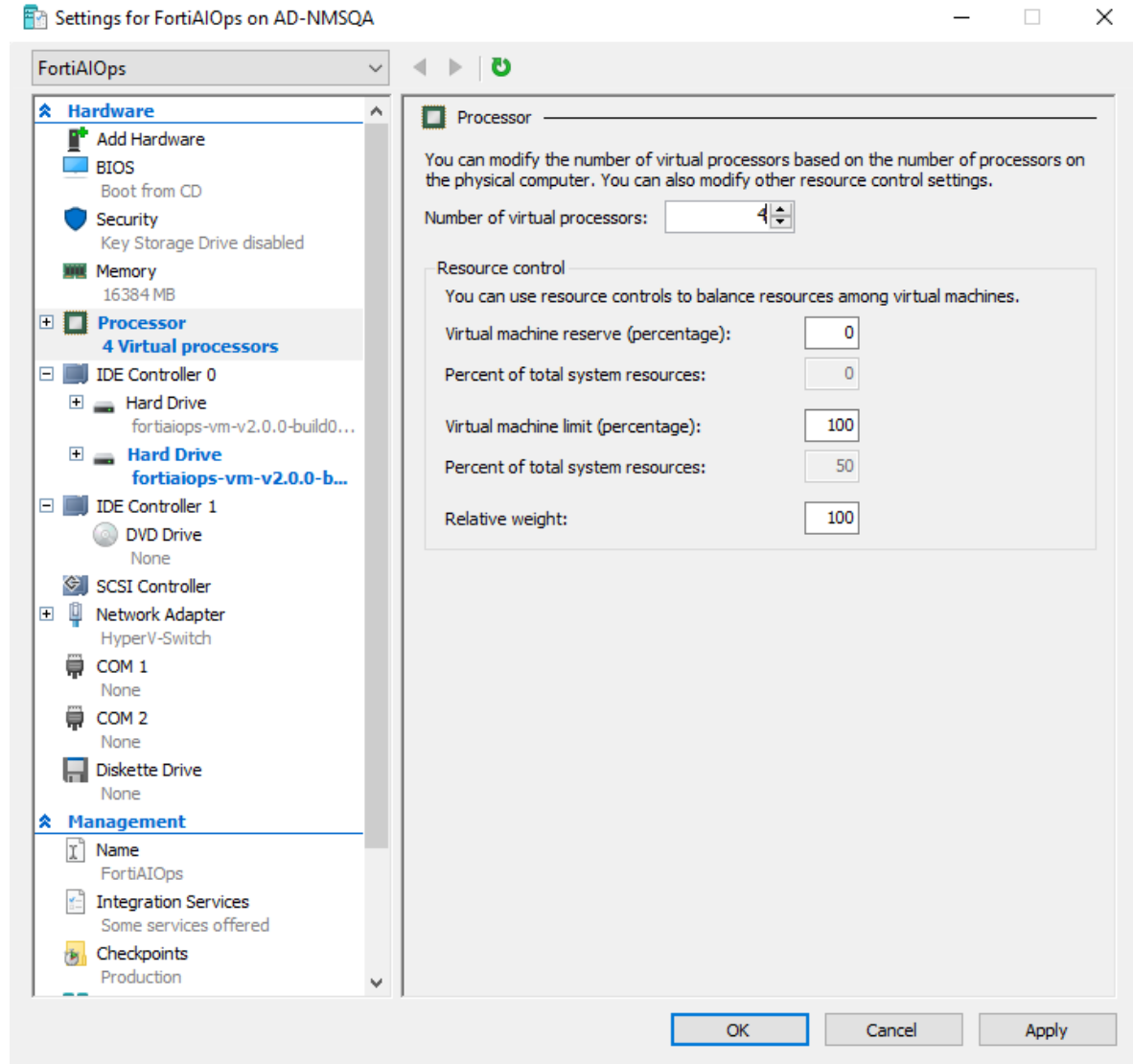
11. Select **IDE Controller 0** under **Hardware** in the left pane. Select **Hard Drive** and click **Add**.



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



13. Select **Processor** under **Hardware** in the left pane. Enter the number of virtual processors based on your [FortiAI Ops configuration](#). Click **Apply**. Click **Ok**.



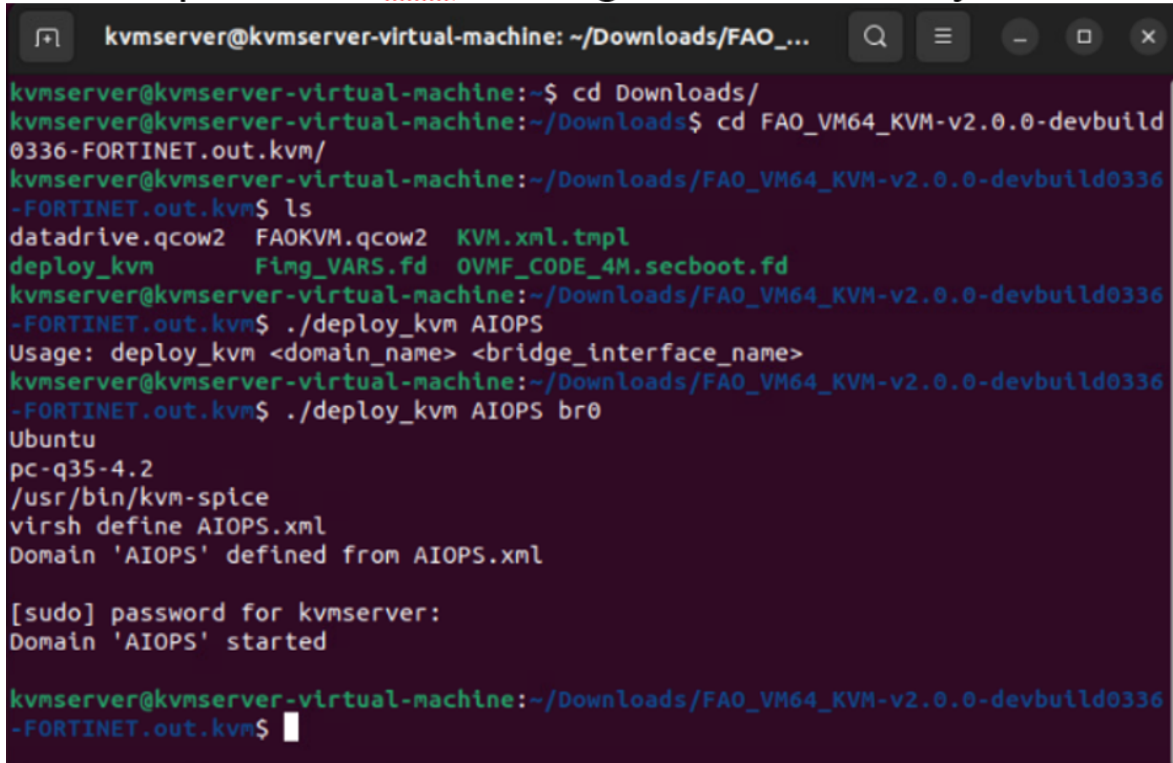
14. Right click on the virtual machine and click **Start**. Once the virtual machine is up and running, launch the console.
15. Perform [post-installation](#) tasks.

Installing FortiAI Ops on KVM

Perform the following steps to deploy FortiAI Ops 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.

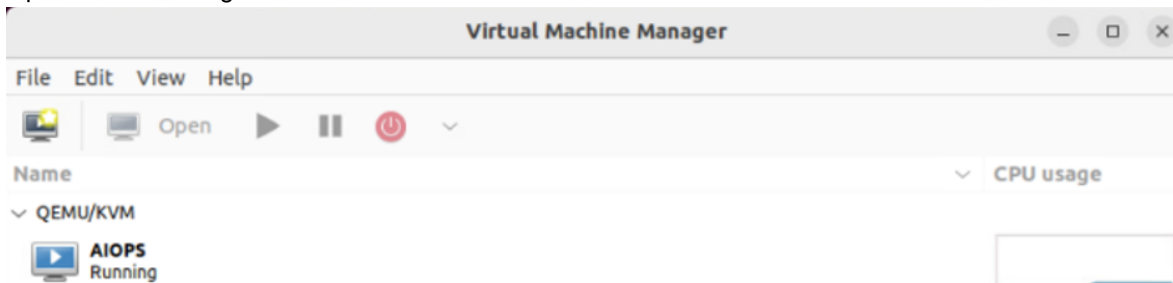


```
kvmserver@kvmserver-virtual-machine: ~/Downloads/FAO_...
kvmserver@kvmserver-virtual-machine:~$ cd Downloads/
kvmserver@kvmserver-virtual-machine:~/Downloads$ cd FAO_VM64_KVM-v2.0.0-devbuild
0336-FORTINET.out.kvm/
kvmserver@kvmserver-virtual-machine:~/Downloads/FAO_VM64_KVM-v2.0.0-devbuild0336
-FORTINET.out.kvm$ 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

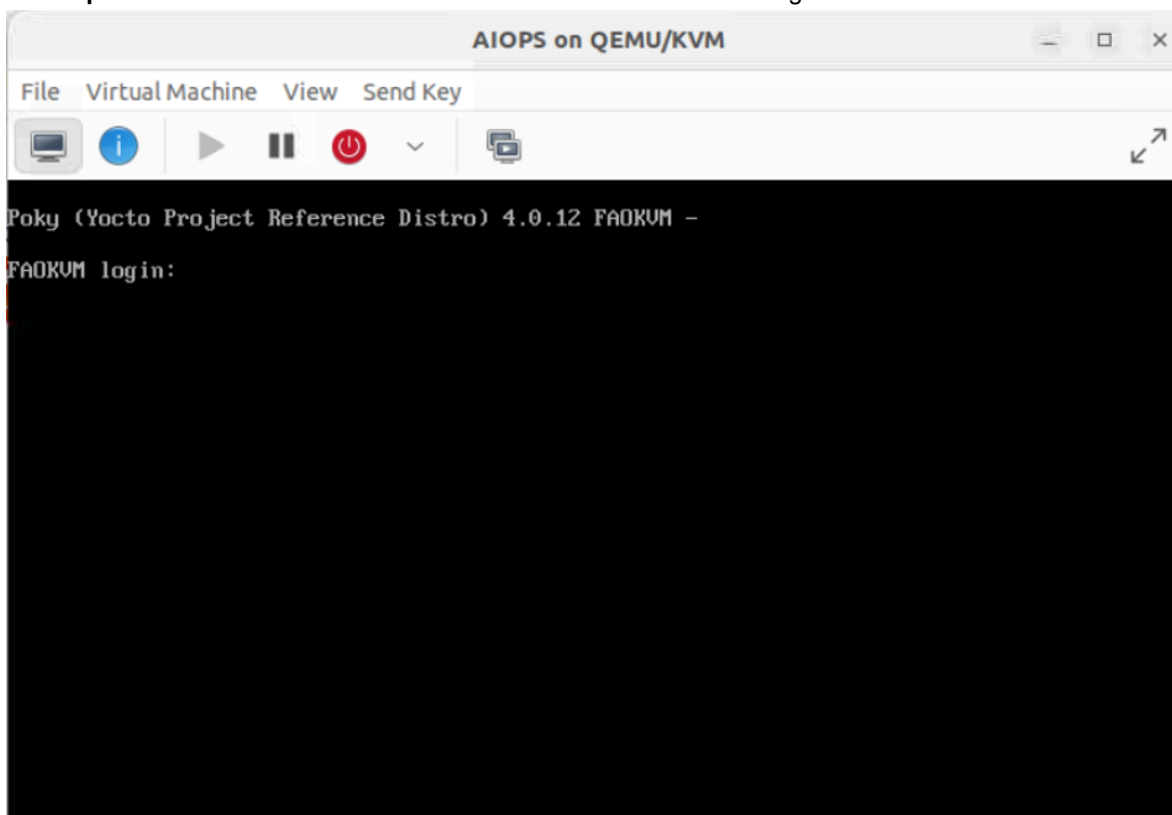
[sudo] password for kvmserver:
Domain 'AIOPS' started

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

4. Open the virt-manager window.



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

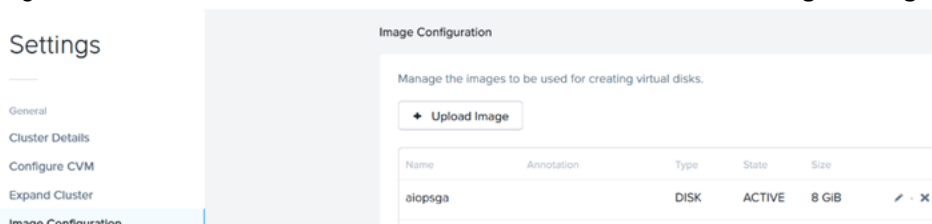


- Perform [post-installation](#) tasks.

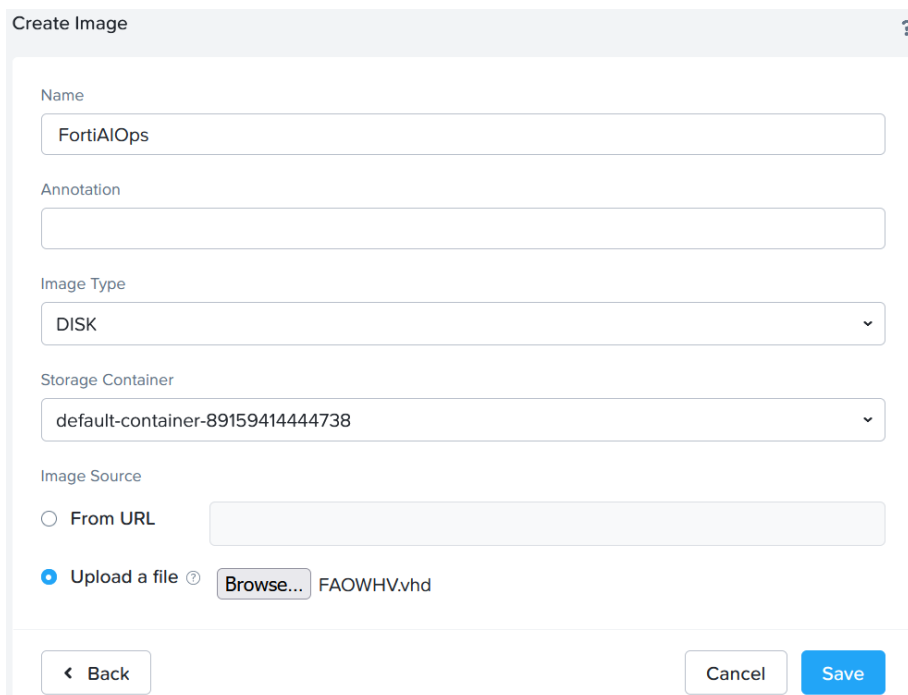
Installing FortiAI Ops on Nutanix

Perform the following steps to deploy FortiAI Ops on Nutanix.

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



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



The screenshot shows the 'Create Image' form with the following fields and values:

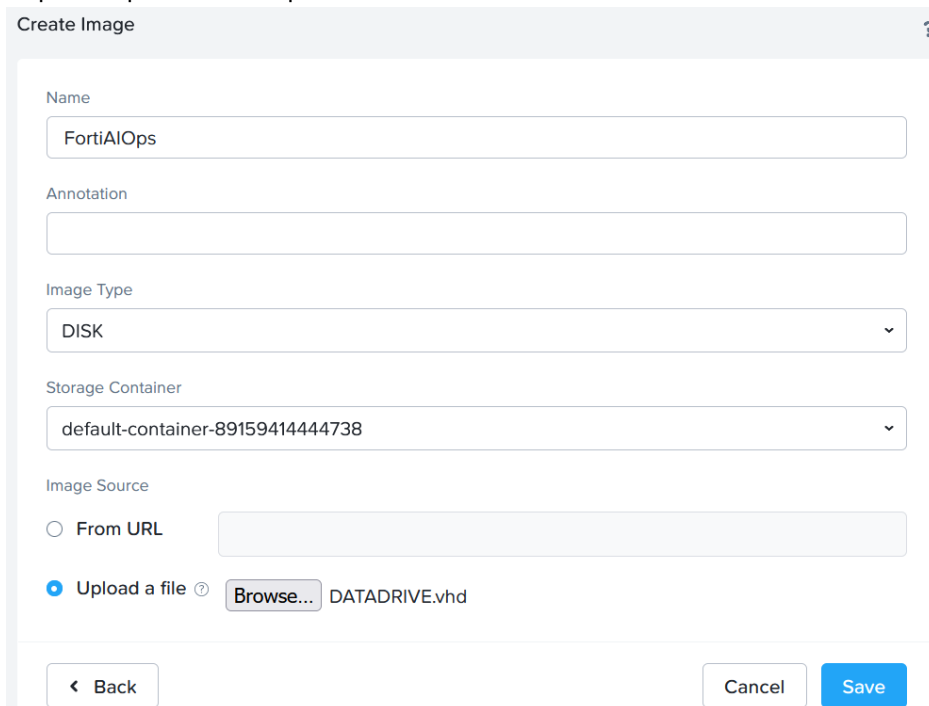
- Name:** FortiAI Ops
- Annotation:** (empty)
- Image Type:** DISK
- Storage Container:** default-container-89159414444738
- Image Source:** ☒ Upload a file (with a help icon) and a 'Browse...' button. The file 'FAOWHV.vhd' is listed next to the button.

At the bottom, there are three buttons: '< Back', 'Cancel', and 'Save'.

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

4. Click **Save**.

5. Repeat steps 3 and 4 to upload *DATADRV.vhd*.



This screenshot is identical to the one above, but the file selected in the 'Image Source' section is 'DATADRV.vhd'.

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



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

? ×

Create VM

General Configuration

Name

Description

Timezone

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

☐ Use this VM as an agent VM

Compute Details

vCPU(s)

Number Of Cores Per vCPU

Memory ?
 GiB

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

Disks + Add New Disk

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

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

- Select the uploaded FortiAI Ops disk **Image** - *FAOWHV.vhd*.

Add Disk?

✕

Type

DISK

Operation

Clone from Image Service

Bus Type

SCSI

Image ?

FortiAI Ops

Size (GiB) ?

500

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

Index

Next Available

Cancel

Add

9. Click **Add**.

10. Add another disk for *DATADRVIVE.vhd* following the previous step.

Note: Ensure to create a new disk for *FAOWHV.vhd* first and then for *DATADRVIVE.vhd*.

11. Add 4 Network Adapters, click **Add New NIC**.

Create NIC?

✕

Subnet Name

fortinet_switch

Network Connection State

Connected

Private IP Assignment

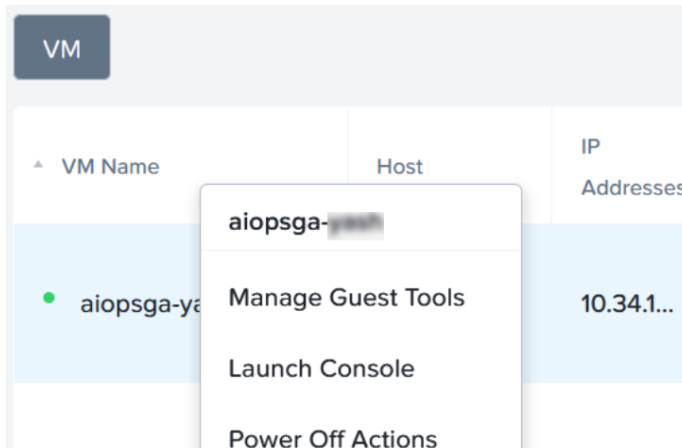
Network address / prefix

NONE

Cancel

Add

12. Power on the VM and launch the console.



13. Configure the FortiAI Ops static IP address on starting the VM. See [Post-installation Tasks](#).

Installing FortiAI Ops on Proxmox

Perform the following steps to deploy FortiAI Ops on the Proxmox KVM platform.

Obtain the Deployment Package

Download the FortiAI Ops deployment package (FAO_VM64_KVM-v[x.x.x]-[build0xxx]-FORTINET.out.kvm.zip) from Fortinet.

Transfer the File to the Proxmox Host

Transfer the downloaded .zip file to your Proxmox server's `/root/` directory using one of the following methods:

Mac / Linux (Using Terminal app)

Use the following built-in SCP command:

```
scp FAO_VM64_KVM-v[x.x.x]-build[yyyy]-FORTINET.out.kvm.zip root@<proxmox-ip>:/root/
```

Where:

- `<proxmox-ip>` with your Proxmox server's IP address (e.g. 192.168.1.50)
- `[x.x.x]` with the correct release number
- `[yyyy]` with the correct build number

Windows (Using WinSCP)

Open WinSCP and connect to your Proxmox host.

- File protocol: `SCP`
- Host name: your Proxmox IP (for example, 192.168.1.50)

- Port: 22
- User name: root
- Password: your Proxmox root password

Drag and drop the .zip file from your local machine into the `/root/` directory on the Proxmox server.

Extract the Package

SSH into your Proxmox host to extract the deployment package.

1. (Optional) If the unzip utility is not installed on your Proxmox host, install it using the following commands:

- a. Update the package list
`apt update`
- b. Install zip and unzip
`apt install zip unzip -y`
- c. Verify the installation
`zip --version`

2. Navigate to the directory and extract the file:

```
cd /root/ unzip FAO_VM64_KVM-vx.x.x-[build0xxx]-FORTINET.out.kvm.zip
```

This will extract the necessary components, including the disk images and deployment scripts.

Prepare the Proxmox Environment

1. Make the Proxmox deployment script executable:

```
chmod +x deploy_pmx
```

2. Identify your Proxmox Storage ID and Network Bridge using the Proxmox web UI:

- Storage ID: Navigate to **Datacenter > Storage** and note the target storage name (for example, local-lvm).
- Network Bridge: Navigate to **Node > Network** and note the bridge name (for example, vmbr0).

Deploy the Virtual Machine

Run the deployment script from the Proxmox shell using the following syntax:

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

where

`<name>` is the name of the VM, for example, fortiaios.

`<volume>` is the target storage ID, for example, local-lvm.

`<bridge>` is the network bridge to use, for example, vmbr0.

`<vmid>` is the ID assigned to the new VM. Proxmox allows you to order virtual machines with their VMID. The default is the next available free ID.

`<cores>` is the number of CPU cores to allocate; the default is 8.

`<memory>` is the amount of RAM to allocate (in MB); the default is 32768 MB.

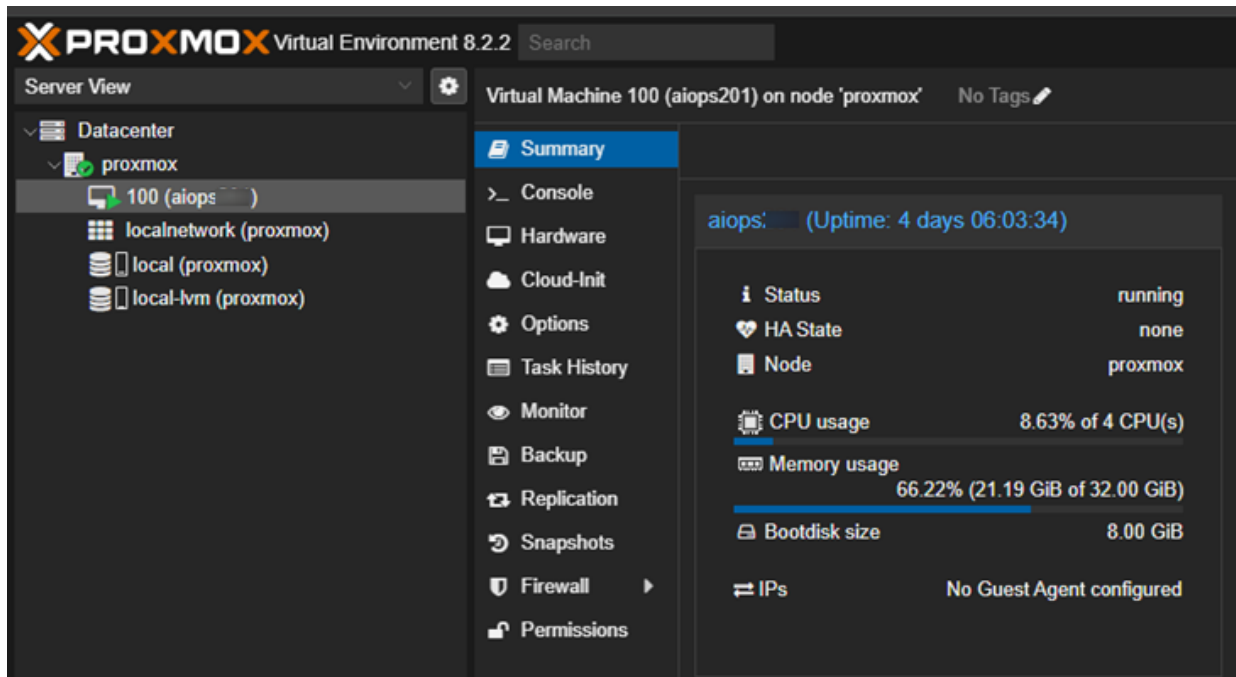
Sample Execution:

```
./deploy_pmx -n fortiaaiops -v local-lvm -b vmbr0 -i 200 -c 8 -m 32768
```

Once the script completes, the FortiAI Ops VM is successfully deployed and will be visible in your Proxmox GUI.

Start the Virtual Machine

After the script completes, navigate to the Proxmox GUI, find the new VM, and click **Start**. Open the **Console** tab to see the boot process.



Configure the Static IP

Once you start the virtual machine (VM), configure the static IP address for FortiAI Ops. After the initial boot sequence completes, a CLI prompt appears. Follow the on screen instructions to assign the management IP address, subnet mask, default gateway, and DNS settings.

Note:

- You will need `root/shell` access to the Proxmox host.
- The storage must have enough free space on the destination storage to deploy and operate the VM.
- If `deploy_pmx` fails, check that the Proxmox tool `qm` is accessible and that the storage and bridge names are spelled exactly right.

Post-installation Tasks

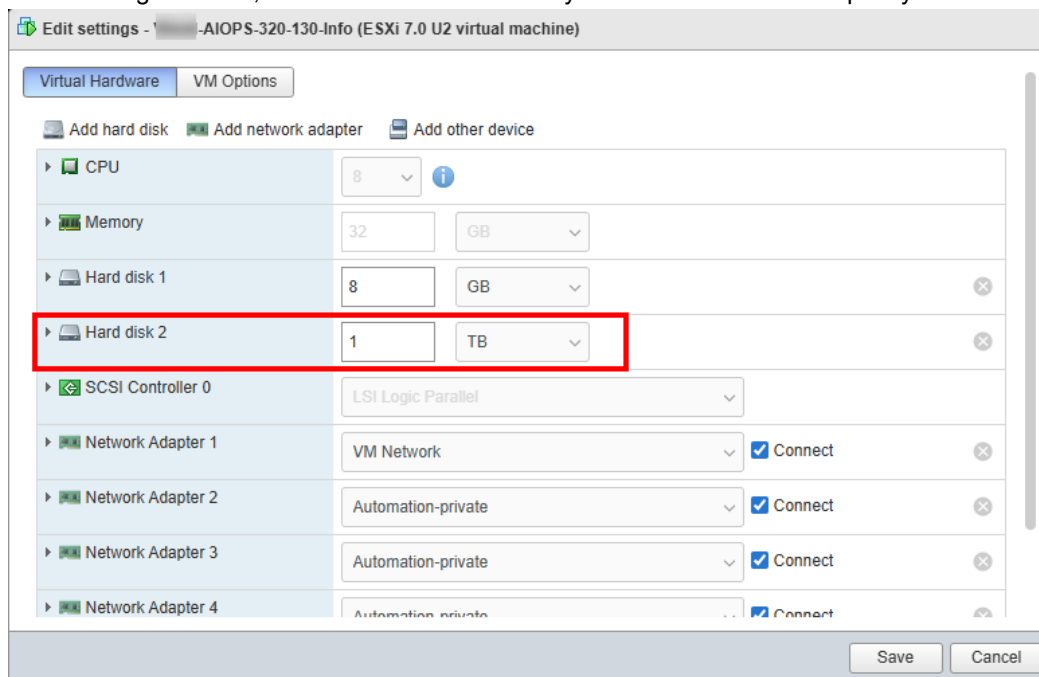
Perform the following steps to access FortiAI Ops after successful installation.

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 FortiAI Ops administrator with username **admin**. Configure the password after the first login.
Note:
 - By default, there is no password for logging into the CLI mode for the first time. However, you are prompted to change the password after logging in.
 - By default, the username for logging into GUI is admin and there is no password.
 - Configuring the CLI password will sync with GUI password
3. Ensure that the IP address is configured properly. Run the `get system interface` command to view the dynamically assigned IP address. Run `config router static` command to assign a static IP address.

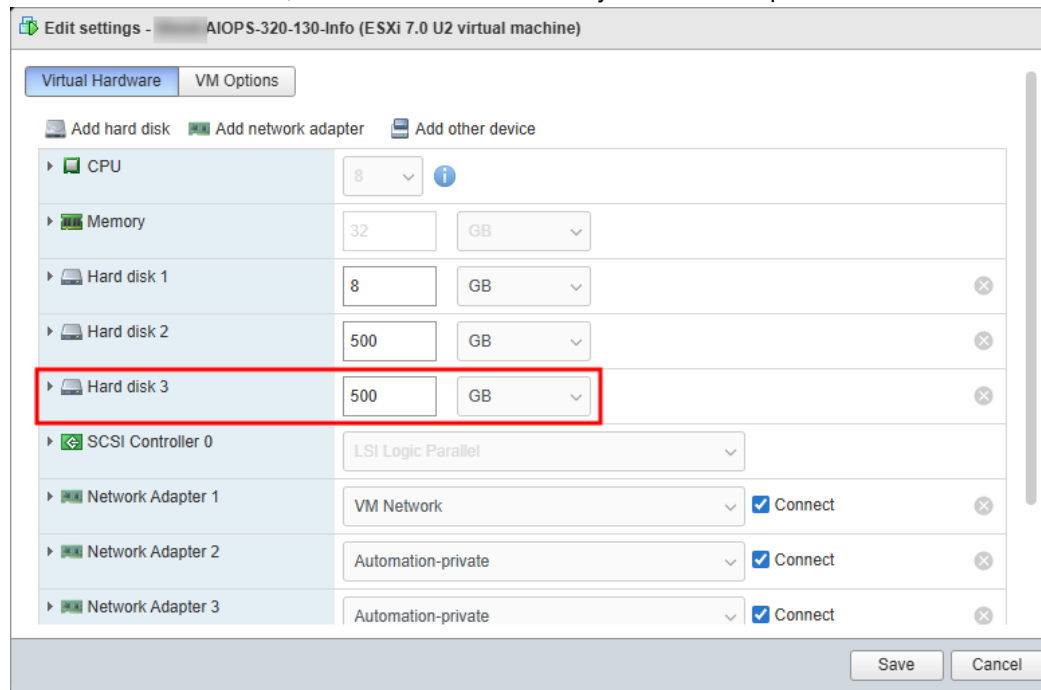
Increasing VM Disk Space

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

1. Log in to your virtual machine management GUI (For example, VMware ESXi).
2. Navigate to the list of virtual machines and select the instance you want to modify.
3. Before making any hardware changes, you must **Shut down** the virtual machine instance to prevent data corruption.
4. Once the VM is off, select the option to **Edit** its settings.
5. In the settings window, find **Hard disk 2** and modify its size to the desired capacity.



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



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

```
FAOESX #
FAOESX #
FAOESX # diagnose hardware deviceinfo disk
TYPE NAME          TRAN LABEL      SIZE FSAAVAIL FSUSE% PATH
disk sda            spi              8G                /dev/sda
part sda1           FORTIBLODR      32M                /dev/sda1
part sda2           fosboot         3G 1.4G 49% /dev/sda2
part sda3           fosboot         3G                /dev/sda3
part sda4           datapartition   2G 1.9G 0% /dev/sda4
disk sdb            spi             1T                /dev/sdb
lvm AppDataVG-AppDataLU 1024G 955.7G 1% /dev/mapper/AppDataVG-AppDataLU
FAOESX #
```

The output shows that the disk sdb is increased to 1 TB in size.

If you have added another hard disk, you will see an output similar to the following:

```
FAOESX # diagnose hardware deviceinfo disk
TYPE NAME          TRAN LABEL      SIZE FSAAVAIL FSUSE% PATH
disk sda            spi              8G                /dev/sda
part sda1           FORTIBLODR      32M                /dev/sda1
part sda2           fosboot         3G 1.4G 52% /dev/sda2
part sda3           fosboot         3G                /dev/sda3
part sda4           datapartition   2G 1.9G 0% /dev/sda4
disk sdb            spi             500G              /dev/sdb
disk sdc            spi             500G              /dev/sdc
lvm AppDataVG-AppDataLU 1000G 937.1G 0% /dev/mapper/AppDataVG-AppDataLU
```

Accessing FortiAI Ops

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

Upgrading FortiAI Ops

You can upgrade FortiAI Ops via the GUI and the CLI.

- **Upgrade via GUI** - Navigate to **System > Upgrade** to upgrade FortiAI Ops. See [Upgrade](#).
- **Upgrade via CLI** - Run the following command to upgrade FortiAI Ops.

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

Deploying FortiAI Ops on Public Cloud Platforms

FortiAI Ops can now be deployed on the following public Cloud platforms.

- [Microsoft Azure](#)
- [Google Cloud Platform](#)
- [Amazon Web Services \(AWS\)](#)
- [Oracle Cloud Infrastructure \(OCI\)](#)

Microsoft Azure

Perform the following steps to deploy FortiAI Ops on Microsoft Azure. For more information on the Azure portal configurations, see the [Azure documentation](#).

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

[Home](#) > [Resource groups](#) >

Create a resource group ...

[Basics](#) [Tags](#) [Review + create](#)

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

Project details

Subscription * ⓘ

Software Development/Engineering

Resource group * ⓘ

fortiaio463 ✓

Resource details

Region * ⓘ

(US) East US

[Review + create](#)

[< Previous](#)

[Next: Tags >](#)

- Create a new **Storage account** or use an existing one from the portal. See [Create a storage account](#).

Home > Storage accounts >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

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

Project details

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

Subscription *

Resource group * [Create new](#)

Instance details

Storage account name *

Region * [Deploy to an edge zone](#)

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

[Previous](#) [Next](#) [Review + create](#)

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

fortiaips01 | Containers

Storage account

Search containers by prefix

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

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

Home > Storage accounts > fortiaips01 | Containers >

fortiaips Container

Overview

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

Location: fortiaips

Search blobs by prefix (case-sensitive)

Add filter

Name	Modified	Access tier	Archive status
☐ FAQ_VM64_AZURE-v2.0.1-devbuild0463-FORTINET.out.vhd	3/26/2024, 12:55:31 PM		

Upload blob

Drag and drop files here or [Browse for files](#)

☐ Overwrite if files already exist

Advanced

Blob type

☒ Upload .vhd files as page blobs (recommended)

Block size

Access tier

Upload to folder

Blob index tags

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

fortiaips Container

Overview

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

Location: fortiaips

Search blobs by prefix (case-sensitive)

Show deleted blobs

Add filter

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
☐ FAQ_VM64_AZURE-v2.0.1-devbuild0463-FORTINET.out.vhd	3/1/2024, 2:57:21 PM			Page blob	8 GiB	Available

3. Create a managed image from the uploaded VHD file. Navigate to **Images > Create** an image in the Azure portal and configure the following settings.

- Select a **Resource group**.
- Enter a **Name** for the image.
- Select the applicable **Region** from the list.
- Set the **OS type** to **Linux**.
- Set the **VM generation** to **Gen 1**.

[Home](#) > [Images](#) > [Create an image](#) >

Create an image ...

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

Project details

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

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Name *

Region * ⓘ

Zone resiliency ⓘ ☐

OS disk

OS type * ⓘ ☐ Windows ☒ Linux

VM generation * ⓘ ☒ Gen 1 ☐ Gen 2

Storage blob * ⓘ [Browse](#)

Account type * ⓘ

Host caching * ⓘ

Encryption

You can encrypt the OS and data disks with a platform-managed or customer-managed key. [Learn more](#)

Key management ⓘ

Data disk

[+ Add data disk](#)

[Review + create](#)

[< Previous](#)

[Next : Tags >](#)

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

[Home](#) > [Virtual machines](#) >

Create a virtual machine

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

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Monitoring](#) [Advanced](#) [Tags](#) [Review + create](#)

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

Project details

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

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region

Availability options

Security type

Image *

[See all images](#) | [Configure VM generation](#)

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

VM architecture ☐ Arm64 ☒ x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount ☐

Size *

[See all sizes](#)

Enable Hibernation (preview) ☐

To enable Hibernation, you must register your subscription. [Learn more](#)

Administrator account

Authentication type ☒ SSH public key ☐ Password

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

Username *

SSH public key source

- Click **See all images** to browse and select the image that was generated in the previous step.
- Click **See all sizes** to select a virtual machine size.

Note: It is recommended to select VM size as 4 vCPU and 32 GB RAM, and the **Local storage** as 0.

Select a VM size ...

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

Showing 17 of 510 VM sizes. | Subscription: Software Development/Engineering | Region: South India | Current size: Standard_E4bs_v5 | Image: fortiaios417 | [Learn more about VM sizes](#) | Group by series

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

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

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

Key pair name *

Inbound port rules

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

Public inbound ports * ☐ None ☒ Allow selected ports

Select inbound ports *

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

Licensing

License type *

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

[Review + create](#) [< Previous](#) [Next: Disks >](#)

<https://portal.azure.com/#>

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

Home > Virtual machines >

Create a virtual machine ...

BasicsDisksNetworkingManagementMonitoringAdvancedTagsReview + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host

Encryption at host is not registered for the selected subscription.
[Learn more about enabling this feature](#)

OS disk

OS disk size

Image default

OS disk type *

Premium SSD (locally-redundant storage)

Delete with VM

Key management

Platform-managed key

Enable Ultra Disk compatibility

Ultra disk is not supported in South India.

Data disks for fortiaio417

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
0	fortiaio417_DataDis...	512	Premium SSD LRS	Read-only	

[Create and attach a new disk](#) [Attach an existing disk](#)

Advanced

Review + create

< Previous

Next : Networking >

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

Home > Virtual machines >

Create a virtual machine

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

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

Network interface

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

Virtual network * [Create new](#)

Subnet * [Manage subnet configuration](#)

Public IP [Create new](#)

NIC network security group ☐ None ☒ Basic ☐ Advanced

Public inbound ports * ☐ None ☒ Allow selected ports

Select inbound ports *

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

Delete NIC when VM is deleted ☐

Delete public IP when VM is deleted ☐

Enable accelerated networking ☐ The selected image does not support accelerated networking.

Load balancing

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

Load balancing options ☒ None ☐ Azure load balancer ☐ Application gateway

Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.

Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.

Review + create < Previous Next : Management >

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

Home > Virtual machines >

Create a virtual machine ...

✓ Validation passed

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

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

fortiaios463	Standard E4 v4
Image	4 vcpus, 32 GiB memory

Basics

Subscription	Software Development/Engineering
Resource group	FortiAI Ops
Virtual machine name	test
Region	South India
Availability options	No infrastructure redundancy required
Security type	Standard
Image	fortiaios463 - Gen1
VM architecture	x64
Size	Standard E4 v4 (4 vcpus, 32 GiB memory)

< Previous Next > **Create**

16. Connect the virtual machine in one for the following methods.

- **Connect via Serial Console** - Select the running virtual machine and then select Serial console in the menu.

FortiAIops440 | Serial console ...

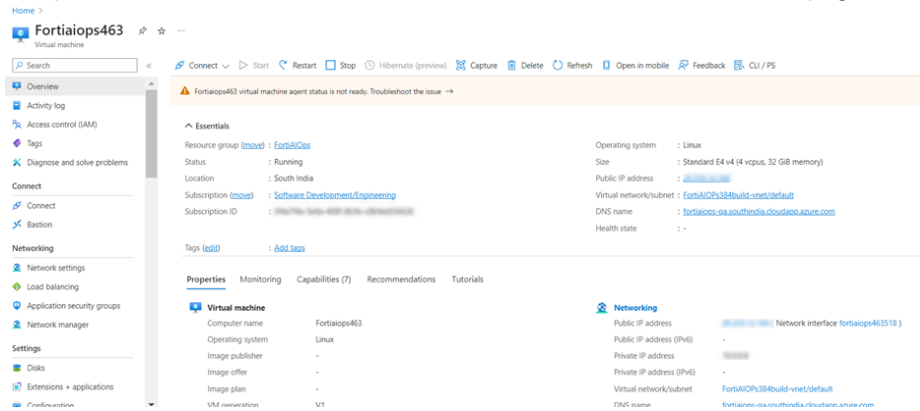
```
[ftaiops]: Fri Mar 15 06:38:12 GMT 2024:: Failed to bring down the docker app
[ftaiops]: Fri Mar 15 06:38:13 GMT 2024:: Failed to bring down the docker app
[ftaiops]: Fri Mar 15 06:38:13 GMT 2024:: Failed to bring down the docker app
[ftapp]: Starting of early services created by ftapp_init.
[ftapp]: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

- **Connect via SSH** - Obtain the public IP address of the virtual machine and use SSH to connect to the virtual machine.

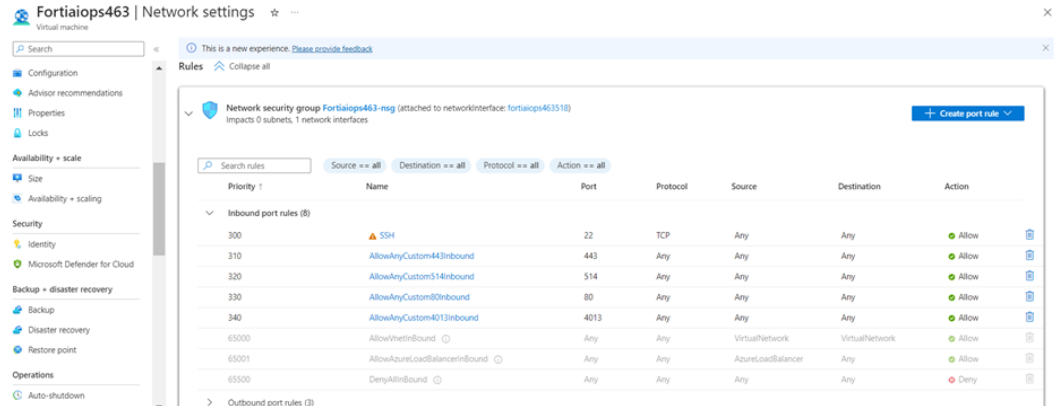
```
ssh admin@<public_IP>
```

Post-installation Tasks

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



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



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

Google Cloud Platform

Perform the following steps to deploy FortiAI Ops on Google Cloud.

- Download the file `FAO_VM64_GCP-v2.0.1-[build0xxx]-FORTINET.out.gcp.zip` from Fortinet and extract it to obtain `FAO_VM64_GCP-v2.0.1-[build0xxx]-FORTINET.out.gcp.tar.gz`.
- Install and setup **gsutil** to access Cloud storage from the CLI using HTTPS. To install **gsutil**, see [Install gsutil](#).
- Alternatively, run the following command to download the Linux 64-bit archive file.

```
curl -O https://dl.google.com/dl/cloudsdk/channels/rapid/downloads/google-cloud-cli-389.0.0-linux-x86_64.tar.gz
```
- Extract the contents of the file to any location on your file system (preferably your Home directory). To replace an existing installation, remove the existing `google-cloud-sdk` directory and then extract the archive to the same location - `tar -xf google-cloud-cli-389.0.0-linux-x86.tar.gz`.

5. Run the `./google-cloud-sdk/install.sh` script (from the root of the folder you extracted the file to).
6. Run `./google-cloud-sdk/bin/gcloud init` to initialize GCP CLI.
7. Upload the file `FAO_VM64_GCP-v2.0.1-[build0xxx]-FORTINET.out.gcp.tar.gz` to the Cloud storage bucket in the GCP CLI.

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

8. Run the following script to create a secure boot image.

```
# bash -x import2gcpimg.sh AIOPSBUILD FAO_VM64_GCP-v2.0.1-devbuild0448-FORTINET.out.gcp.tar.gz aiops-gcp.
```

where, `IMAGE_NAME` = `[FortiAIops build]`, `SOURCE_FILE` = `[FortiAIops image file name]`, and `BUCKET_NAME` = `aiops-gcp`.

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

```

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

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

```

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

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

← Create an instance

New VM instance
Create a single VM instance from scratch

New VM instance from template
Create a single VM instance from an existing template

New VM instance from machine image
Create a single VM instance from an existing machine image

Marketplace
Deploy a ready-to-go solution onto a VM instance

Name *
imageaiops448

MANAGE TAGS AND LABELS

Region *
us-central1 (Iowa)
Region is permanent

Zone *
us-central1-a
Zone is permanent

Machine configuration

☒ General purpose ☐ Compute optimized ☐ Memory optimized ☐ Storage optimized **NEW** ☐ GPUs

Machine types for common workloads, optimized for cost and flexibility

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

CREATE **CANCEL** **EQUIVALENT CODE**

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

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

PRESET **CUSTOM**

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

	vCPU	Memory
	4 (2 cores)	16 GB

CPU platform
Automatic

vCPUs to core ratio
2 vCPUs per core

Visible core count
2 cores

ADVANCED CONFIGURATIONS

Availability policies
VM provisioning model
Standard

Choose "Spot" to get a discounted, preemptible VM. Otherwise, stick to "Standard". [Learn more](#)

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

Firewall ?

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

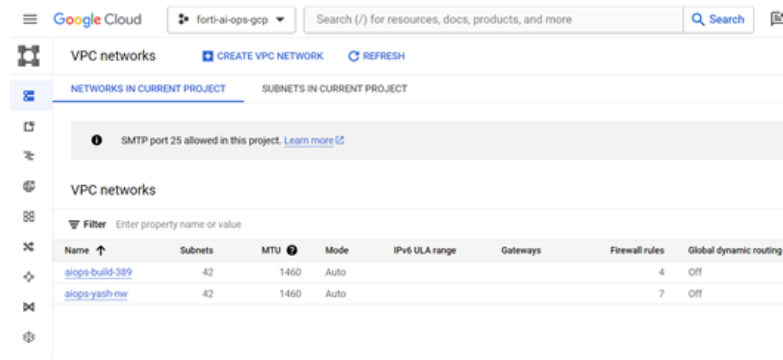
- ☒ Allow HTTP traffic
- ☒ Allow HTTPS traffic
- ☐ Allow Load Balancer Health Checks

- Click **Advanced options** to configure networking, disk and security parameters for the instance.

- Set the **Network interface card** to **VirtIO**.
- Select the Virtual Private Cloud (VPC) in the **Network interfaces**.

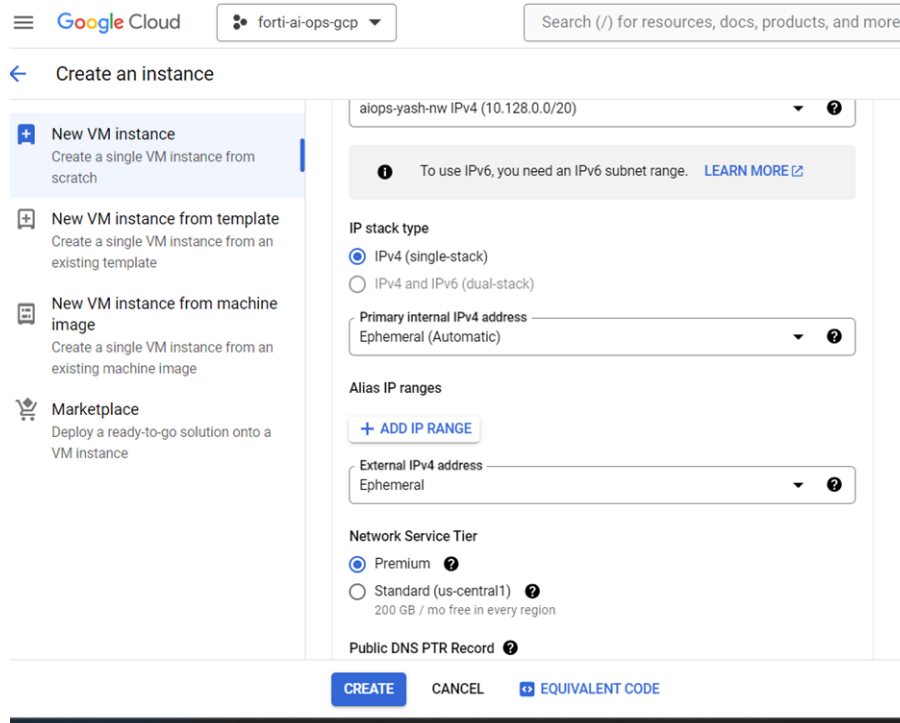
Note: Ensure that you create VPC networks to use as network interfaces for your instance, and provide

the IP address from specified subnets. To create and use a VPC network, see [Create and manage VPC networks](#).



- Select other network parameters such as IP stack, primary Internal IPv4 address, and external IPv4 address as depicted in this image.

Note: You can select the external IPv4 address as Ephemeral (automatic /dynamic or static IP address.). To create external IPv4 addresses for GCP, see [Reserve a static external IP address](#).



13. Add another hard disk. In the **Create an instance** page, select **Add New Disk** and configure the following.

- Enter a disk **Name**.
- Set the **Disk source type** to **Blank disk**.
- Set the **Disk type** to **Standard persistent disk**.
- Set the disk **Size** to 100 GB

Note: The minimum recommended disk size is 100 GB.

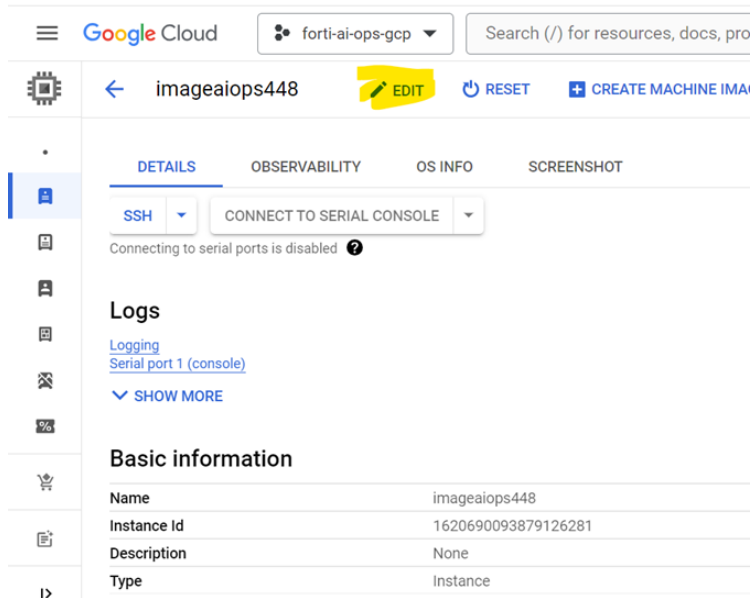
14. Click **Save**.

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

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

17. After successful installation, enable the serial console.

- Select the instance in the **VM instances** page.



Google Cloud fort-ai-ops-gcp Search (/) for resources, docs, pro

imageaiops448 EDIT RESET CREATE MACHINE IMAGE

DETAILS OBSERVABILITY OS INFO SCREENSHOT

SSH CONNECT TO SERIAL CONSOLE

Connecting to serial ports is disabled

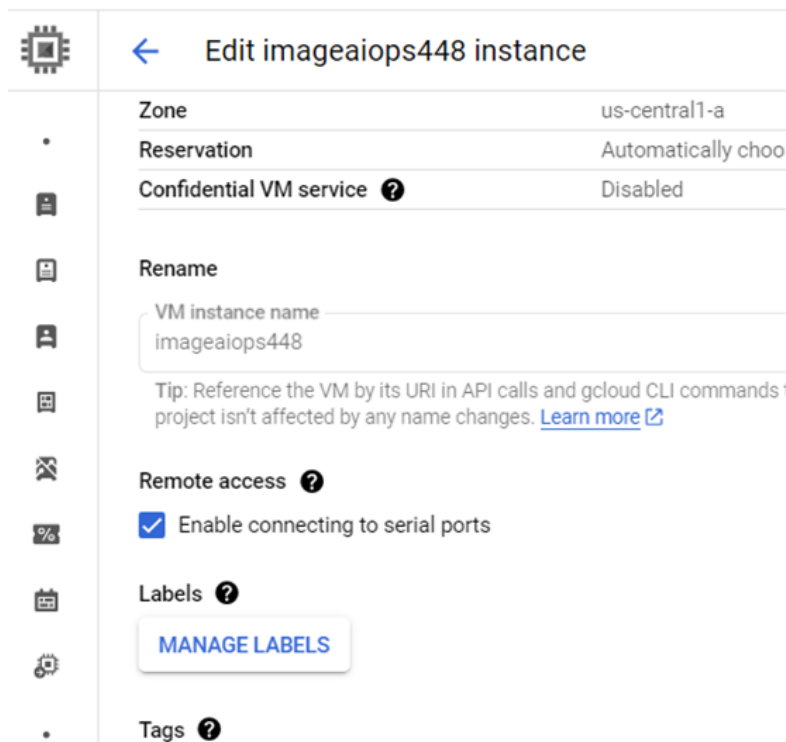
Logs

[Logging](#)
[Serial port 1 \(console\)](#)
[SHOW MORE](#)

Basic information

Name	imageaiops448
Instance Id	1620690093879126281
Description	None
Type	Instance

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



Edit imageaiops448 instance

Zone us-central1-a

Reservation Automatically choose

Confidential VM service Disabled

Rename

VM instance name
imageaiops448

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

Remote access

☒ Enable connecting to serial ports

Labels

[MANAGE LABELS](#)

Tags

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

- 80:80/tcp

Protocols and ports ?

☐ Allow all

☒ Specified protocols and ports

☒ TCP

Ports

E.g. 20, 50-60

☒ UDP

Ports

E.g. all

☐ Other

Protocols

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

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

18. Connect the VM instance and login.

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

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

FAOGCP #
FAOGCP # get system status
Platform:          FAO_VM64_GCP (Debug)
Version:           FAO_VM64_GCP v2.0.1,build0448,240310 (Debug)
Architecture:     64-bit
Serial-Number:    FAOGCP
Hostname:          FAOGCP
Branch point:     0448
Uptime:           0 days, 0 hours, 20 minutes
Last reboot:      Thu Mar 28 11:44:05 GMT 2024
System time:      Thu Mar 28 12:04:24 GMT 2024
SystemID:         fb370651-3cc5-c390-a185-13b7b7b7b7b7

FAOGCP #
```

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

instance.

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

FAOGCP #
FAOGCP #
FAOGCP # get system interface
== [ port1 ] (2024-03-28 11:44:14)
type: physical    mode: dhcp    ip: 10.128.0.8/32    allowaccess: https ping ssh http

Number of items: 1

FAOGCP #
```

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

Amazon Web Services (AWS)

Perform the following steps to deploy FortiAI Ops on AWS.

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

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

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

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

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

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

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

```
cat <<EOF > role-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::$s3BucketName",
        "arn:aws:s3:::$s3BucketName/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
EOF
```

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

For more information, see [Importing a VM as an Image](#).

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

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

Permissions policies (3)

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

Filter by Type: All types

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

IAMtoCreatePolicy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "iam:CreateRole",
9         "iam:PutRolePolicy"
10      ],
11      "Resource": "arn:aws:iam::250424965647:role/*"
12    }
13  ]
14 }
```


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

The screenshot displays the AWS IAM console interface. At the top, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Security credentials' tab is selected. Below this, there are three main sections: 'Console sign-in', 'Multi-factor authentication (MFA)', and 'Access keys'. The 'Console sign-in' section shows a 'Console sign-in link' and a 'Console password' status. The 'Multi-factor authentication (MFA)' section shows a message indicating that no MFA devices are assigned and provides an 'Assign MFA device' button. The 'Access keys' section shows a table with one active access key, including details like 'Description', 'Status', 'Created', 'Last used', and 'Last used region'.

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

```
check_S3 $s3BucketName

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

import_image
```

6. Extract the file `FAO_VM64_AWS-v2.0.1-[build01xx]-FORTINET.out.aws.zip`. Post extraction, you have the VHD file and the import script.
 - a. VHD - `FAO_VM64_AWS-v2.0.1-[build01xx]-FORTINET.out.vhd`
 - b. Import script - `import2awsimg.sh`
7. Run the `import2awsimg.sh` script to import the VM.

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

```
virtual-machine:~/Downloads/test$ bash -x import2awsimg.sh FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd aiopsqa
+ '[' 2 -gt 1 ']'
+ imageFile=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ s3BucketName=aiopsqa
+ '[' '!' -f FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd ']'
+ check_S3 aiopsqa
+ type aws
+ aws s3 ls s3://aiopsqa
+ '[' 0 -ne 0 ']'
+ import_image
++ basename FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ imageName=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ amIName=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out
+ echo 'Upload image file to S3..'
Upload image file to S3..
+ aws s3 cp FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd s3://aiopsqa/FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
upload: ./FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd to s3://aiopsqa/FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ cat
+ echo 'Start import image file as snapshot..'
Start import image file as snapshot..
++ aws ec2 import-snapshot --description 'fimg aws' --disk-container file://container.json
++ awk -F "" '{if($2=="ImportTaskId")print $4}'
+ import_task_id=import-snap-05a78f80bdd0517b1
+ '[' -z import-snap-05a78f80bdd0517b1 ']'
+ echo import-snap-05a78f80bdd0517b1
import-snap-05a78f80bdd0517b1
+ true
++ aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-05a78f80bdd0517b1
```

```
+ amiId=ami-038a0845e0f322b35
+ '[' -z ami-038a0845e0f322b35 ']'
+ aws ec2 create-tags --resources ami-038a0845e0f322b35 --tags Key=Name,Value=FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out
+ echo 'Register AMI done..'
Register AMI done..
+ echo 'AMI ID: ami-038a0845e0f322b35'
AMI ID: ami-038a0845e0f322b35
+ echo 'AMI NAME: FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out'
AMI NAME: FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out
+ rm -f block_device_mappings.json container.json
```

Note:

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

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

Name	AMI name	AMI ID	Source	Owner	Visibility	Status
FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	ami-038a0845e0f322b35	250424965647/FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	250424965647	Private	Available
FA0_VM64_AWS-v2.0.1-devbuild0446-FORTINET.out	FA0_VM64_AWS-v2.0.1-devbuild0446-FORTINET.out	ami-0028453cb35ce0848	250424965647/FA0_VM64_AWS-v2.0.1-devbuild0446-FORTINET.out	250424965647	Private	Available

AMI ID: ami-038a0845e0f322b35 (FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out)

Details		Permissions		Storage		Tags	
AMI ID	ami-038a0845e0f322b35 (FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out)	Image type	machine	Platform details	Linux/UNIX	Root device type	EBS
AMI name	FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	Owner account ID	250424965647	Architecture	x86_64	Usage operation	RunInstances
Root device name	/dev/sda1	Status	Available	Source	250424965647/FA0_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	Virtualization type	hvm
Boot mode	uefi	State reason	-	Creation date	Mon Mar 25 2024 18:21:51 GMT+0530 (India Standard Time)	Kernel ID	-
Description	-	Product codes	-	RAM disk ID	-	Deprecation time	-

9. Add **Name and tags** for the instance, select the **Instance type**, set the **Key pair**, and configure the **Network settings** based on your requirement. Select the required hard disk size in **Configure storage**. The default size of disk storage 2 is 10 GB, modify the size as per your requirement. Click **Launch instance**.

Launch an instance [Info](#)
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

 [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

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

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

Recents **My AMIs** Quick Start

☒ Owned by me ☐ Shared with me

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

FAO_VM64_AWS-v2.1.0-build0313-FORTINET.out
ami-0472535e8614aad1d
2023-03-08T10:22:20.231Z Virtualization: hvm ENA enabled: true Root device type: ebs Root mode: userf

Description

-

Architecture	AMI ID
x86_64	ami-0472535e8614aad1d

Instance type [Info](#) [Get advice](#)

Instance type

t3.xlarge
Family: t3 8 vCPU 32 GiB Memory Current generation: true On-Demand RHEL base pricing: 0.448 USD per Hour
On-Demand Linux base pricing: 0.5328 USD per Hour On-Demand Ubuntu Pro base pricing: 0.5468 USD per Hour
On-Demand SUSE base pricing: 0.4578 USD per Hour On-Demand Windows base pricing: 0.48 USD per Hour

☒ All generations [Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Key pair (login) [Info](#)

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

Key pair name - required

 [Create new key pair](#)

Network settings [Info](#) [Edit](#)

Configure storage [Info](#) [Advanced](#)

1x 17 GiB gp2 Root volume, Not encrypted

1x 500 GiB gp2 EBS volume, Not encrypted

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

[Add new volume](#)

Summary

Number of instances [Info](#)

1

Software Image (AMI)
FAO_VM64_AWS-v2.1.0-build0313-...[read more](#)
ami-0472535e8614aad1d

Virtual server type (instance type)
t3.xlarge

Firewall (security group)
-

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

[Cancel](#) [Launch Instance](#) [Preview code](#)

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

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

```

FA0AWS #
config          Configure object.
get             Get dynamic and system information.
show           Show configuration.
diagnose        Diagnose facility.
execute         Execute static commands.
exit           Exit the CLI.
full-configuration Show full configuration.

FA0AWS-AWS-Vinod # show
config system global
    set hostname FA0AWS-AWS-Vinod
end
config system interface
    edit port1
        set type physical
        set mode dhcp
        set allowaccess https ping ssh http
        config ipv6
        end
    next
end
config router static
end
config router static6
end
config system dns
end
config system ntp
end
config system admin
    edit admin

```

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

Oracle Cloud Infrastructure (OCI)

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

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

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

Object Storage & Archive Storage

Buckets

List scope

Compartment

forti-ai-ops-qa-team

fortinetoracelcloud1 (root)/forti-ai-ops-qa-team

Service logs [Manage logs](#)

Resources: 1 (2 total logs) ⓘ

Logs enabled: 0

Logs not enabled: 2

Tag filters [add](#) | [clear](#)

no tag filters applied

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

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

[Create Bucket](#)

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

Showing 1 item < 1 of 1 >

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

ORACLE Cloud

Cloud Classic >

Search resources, services, documentation, and Marketplace

US West (Phoenix) v

Approximate Object Count: 0

Approximate Size: 0 bytes ⓘ

Uncommitted Multipart Uploads

Uncommitted Multipart Uploads

Resources

Objects

[Upload](#) [More Actions](#)

☐ **Name**

Upload Objects [Help](#)

Object Name Prefix: Optional

fortiops

Storage Tier

Standard

Choose Files from your Computer

Drop files here or [select files](#)

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

1 files, 1.26 GiB total

[Show Optional Response Headers and Metadata](#)

[Upload](#) [Cancel](#)

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

Import image

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

Name: **fortiaios**

Operating system: **Oracle Linux**

☒ Import from an Object Storage bucket
☐ Import from an Object Storage URL

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

Object name: **fortiaiosFAQ_VM94_OCI-v2.1.0-daily-devbuild0001-FORTINET.out.vmdk**

Image type:
☒ VMDK
☐ OCOW2

Import image Cancel

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

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

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

Name	State	Public IP	Private IP	Shape	OCPU count	Memory (GB)	Availability domain	Fault domain	Created
aiops-devops	Stopped			VM.Standard.E5.Flex	4	16	AD-1	FD-3	Fri, Oct 4, 2024, 09:24:04 UTC
aiops-final	Stopped			VM.Standard.E5.Flex	4	16	AD-1	FD-2	Thu, Oct 3, 2024, 07:48:40 UTC
aiops55	Terminated			VM.Standard.E5.Flex	4	16	AD-1	FD-3	Thu, Oct 3, 2024, 03:31:55 UTC

0 selected Showing 3 items < 1 of 1 >

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

Create compute instance

Image and shape

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

Image

aiops-devops

Change image

Shape

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

Change shape

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

The screenshot displays the AWS Management Console interface for an instance named 'aiops-final'. The left sidebar shows the 'Resources' section with 'Attached block volumes' selected. The main content area is titled 'Attach block volume' and includes a 'Volume' section with a dropdown menu showing 'aiops_final'. Below this, the 'Attachment type' section has radio buttons for 'Recommended' (selected), 'Custom', and 'Use in-transit encryption'. The 'Access' section has radio buttons for 'Read/write' (selected), 'Read/write - shareable', and 'Read-only - shareable'. The instance details on the left show it is in the 'Running' state.

12. Reboot the instance after attaching the volume.

Deploying FortiAI Ops on Hardware Platforms



By default, the hardware does not include any subscription or device support. These services must be purchased separately. For more information, see the [FortiAI Ops Ordering Guide](#).

FortiAI Ops can be deployed on the following hardware platform:

- [Deploying FortiAI Ops 500G \(FAO-500G\)](#)
- [Deploying FortiAI Ops 100G \(FAO-100G\)](#)

Deploying FortiAI Ops 500G (FAO-500G)

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

- [Initial Configuration](#)
- [Accessing the GUI](#)
- [Supported Devices](#)

Initial Configuration

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

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



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

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

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

Accessing the GUI

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

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

`https://<fortiaips_server_IP>`

Replace `<fortiaips_server_IP>` with the static IP address you configured.

- Log in using the default GUI credentials. Enter the username as admin. There is no password for the initial login.

Supported Devices

The following are the maximum devices supported in FortiAI Ops 500G hardware.

Maximum device count	Supported Mode
- FortiGates - 1000 - FortiSwitches - 3000 - FortiExtenders - 1000 - FortiAPs - 6000 - Clients - 25000	AI Insights and Monitoring
- FortiGates - 2500 - FortiSwitches - 7500 - FortiExtenders - 2500 - FortiAPs - 15000 - Clients - 60000	Monitoring only

FortiAI Ops supports RAID levels 0, 1, 5, and 10. The default configuration uses RAID 5 for HDDs and RAID 1 for SSDs. The following are the storage capacities for RAID levels in the default and maximum FortiAI Ops 500G hardware configurations.

RAID Level	FortiAI Ops 500G Hardware Configuration	
	Default (4 HDDs, 2 SSDs)	Maximum (8 HDDs, 4 SSDs)
RAID 0	18 TB	36 TB
RAID 1	9.0 TB	18 TB
RAID 5	13 TB	31 TB
RAID 10	9.0 TB	18 TB

Note:

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

Deploying FortiAI Ops 100G (FAO-100G)

The FAO-100G hardware platform comes with FortiAI Ops pre-installed. Perform the following steps to deploy and configure the device.

- [Initial Configuration](#)
- [Accessing the GUI](#)
- [Supported Devices](#)

Initial Configuration

After setting up and mounting the appliance on the rack, connect to the FortiAI Ops 100G CLI using the console port and perform the following steps. See, *FortiAI Ops 100G Quick Start Guide*.

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



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

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

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

Accessing the GUI

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

1. Open a web browser and enter the following URL.
`https://<fortiaios_server_IP>`
 Replace `<fortiaios_server_IP>` with the static IP address you configured.
2. Log in using the default GUI credentials. Enter the username as admin. There is no password for the initial login.

Supported Devices

The following are the maximum devices supported in FortiAI Ops 100G hardware.

Maximum device count	Supported Mode
• FortiGates - 30 • FortiSwitches - 90 • FortiExtenders - 30 • FortiAPs - 180 • Clients - 3000	AI Insights and Monitoring

Maximum device count	Supported Mode
• FortiGates - 200 • FortiSwitches - 600 • FortiExtenders - 200 • FortiAPs - 1200 • Clients - 10000	Monitoring only

Command Line Interface (CLI) Reference

The following commands are supported for FortiAIOps.

- [Configuration Commands](#)
- [Show Commands](#)
- [Diagnostic Commands](#)
- [Management Commands](#)
- [System Information](#)
- [Diagnostic Tool Commands](#)

Configuration Commands

The following commands are available to configure FortiAIOps.

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

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

Command	Parameters	Description
	lldp-transmission	LLDP is enabled by default on all interfaces, global and per interface settings. Run the following commands to manage LLDP. <pre>config system global set lldp-transmission enable <enable LLDP> disable <disable LLDP></pre>

Show Commands

The following commands can be used for viewing configuration information.

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

Diagnostic Commands

The following commands are used to diagnose and troubleshoot issues.

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

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

Command	Parameters	Description
	<code>fsck harddisk</code>	Check and repair the file system, then reboot the system.
	<code>raid hwinfo</code>	Displays raid controller information.
	<code>raid hwinfodetail</code>	Displays detailed raid controller information.
	<code>raid migrate</code>	Migrate to a new disk.
	<code>raid rebuild</code>	Rebuild the existing disk.
	<code>disk attributes</code>	Displays vendor specific Self-Monitoring, Analysis, and Reporting Technology (SMART) attributes.
	<code>disk errors</code>	Displays SMART error logs.
	<code>disk health</code>	Displays SMART health status.
	<code>disk info</code>	Displays SMART information.
diagnose debug application location	0	Reset: Resets the logging level in the backend.
	1	Error: Logs only critical failures or errors.
	2	Warn: Logs errors and potential issues (warnings).
	3	Info: Logs standard operational events.
	4	Debug: Logs detailed information useful for troubleshooting specific bugs.
	5	Trace: Traces the code execution path.

Management Commands

The following enable some management and other operations in FortiAI Ops.

Command	Parameters	Description
execute	?	Displays the various parameters available for this command.

Command	Parameters	Description
	<code>date <YYYY-MM-DD></code>	Set the date in the <i>YYYY-MM-DD</i> format.
	<code>time <HH:MM:SS></code>	Set the time in the <i>HH:MM:SS</i> format.
	<code>factoryreset reboot</code>	Reset to the factory default settings and reboot the system.
	<code>factoryreset shutdown</code>	Reset to the factory default settings and shutdown the system.
	<code>formatlogdisk</code>	Format the log disk.
	<code>ping <destination></code>	Ping the host name or IPv4 address.
	<code>traceroute <destination></code>	Traceroute of the host name or IPV4 address.
	<code>reboot</code>	Reboot the system.
	<code>shutdown</code>	Shut down the device.
	<code>backup config ftp <path> <server fqdn ipaddr>[:port] [ftp_user] [ftp_passwd]</code>	Creates a remote backup of the configuration file from an FTP server.
	<code>backup config tftp <filename> <server fqdn ipaddr></code>	Creates a remote backup of the configuration file from a TFTP server.
	<code>restore image ftp <filename string> <ftp server>[:port] [ftp_user] [ftp_passwd]</code>	Restores the firmware image from an FTP server using specific details.
	<code>restore image tftp <filename string> <tftp server></code>	Restores the firmware image from a TFTP server.
	<code>dns-no-domain</code>	The <i>DNS No Domain</i> events are disabled in FortiAI Ops, by default. Run the following commands to enable these events. <pre> execute dns-no-domain disable <disable the events> enable <enable the events> status <show the current setting> </pre>

Command	Parameters	Description
	<code>sensor list</code>	Displays sensor list and status from IPMI.
	<code>format disk 0</code>	Create RAID 0 and format disk.
	<code>format disk 1</code>	Create RAID 1 and format disk.
	<code>format disk 5</code>	Create RAID 5 and format disk.
	<code>format disk 10</code>	Create RAID 10 and format disk.

System Information

The following commands information related to the system configurations.

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

Diagnostic Tool Commands

Use the following command to run diagnostics using the CLI:

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

Dashboard

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

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

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

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

Dashboard Filters

Dashboard widget filters and configurations are automatically saved to your user profile, ensuring your personalized view remains consistent across sessions. These settings (applied filters, widget sizing, and positioning) persist through page reloads, logouts, browser changes, and when switching between ADOMs. Since these configurations are stored at the user level, your preferences are unique to your account and are not affected by global navigation or other user activities.

Adding a Widget to the Dashboard

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

To add a widget to the dashboard:

1. Select the dashboard you want to modify.
2. Click **Add Widget** to add required widgets from the widget library.
3. In the **Manage Dashboard Widgets** pane, hover on the widget name to select the required widget and click +.
For more information on widget library, see [Managing Dashboard Widgets](#)
4. Click **Close** to close the pane once the widgets are selected.
5. Click **Reset dashboard layout** to clear all the widgets added to the dashboard.

Summary

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

The following charts are available:

- [System Information](#)
- [System Resource Summary](#)
- [Summary](#)
- [Acknowledged Events](#)
- [Overall Network Health](#)
- [Top 5 Problematic Devices](#)
- [Impacted Clients Trend](#)
- [FortiGates](#)
- [FortiGate Events](#)
- [FortiGates CPU Usage and FortiGates Memory Usage](#)
- [High Latency FortiGates](#)

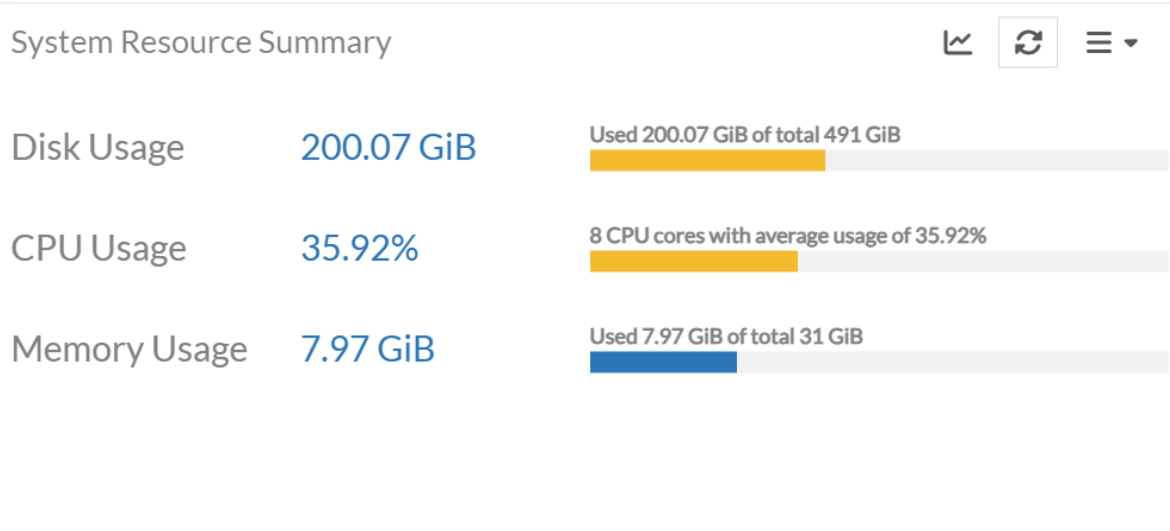
System Information

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

System Information		 
Host Name	FAOESX	
Firmware	v3.0.0- 	
System ID	97d24c 	
System Time	2025/06/09 20:14:20	
Uptime	2d:21h:36m:43s	
IP Address	10.32.8.25	

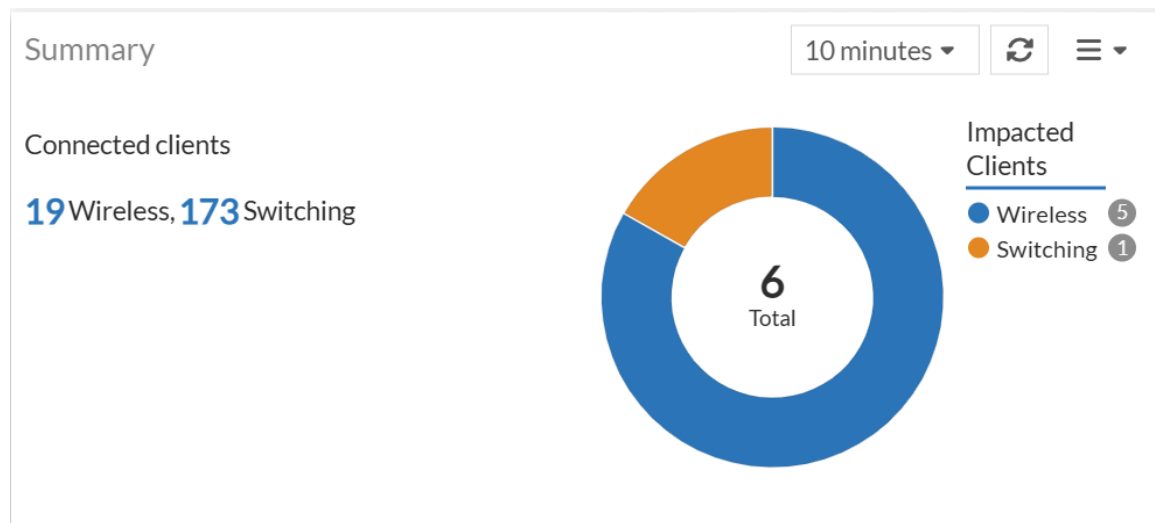
System Resource Summary

This widget provides an overview of the current system resource usage for FortiAIOps. The statistics include the total available and used disk space (HDD and SSD), the number of CPU cores used and the average usage, and total available and used memory. Click on the trends icon to view the resource usage summary; filter data based on the selected duration or customized time slot. You can select a time window or define a **Custom range**. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**. The minimum, maximum, and average values are displayed when a time interval of more than 6 hours is selected.



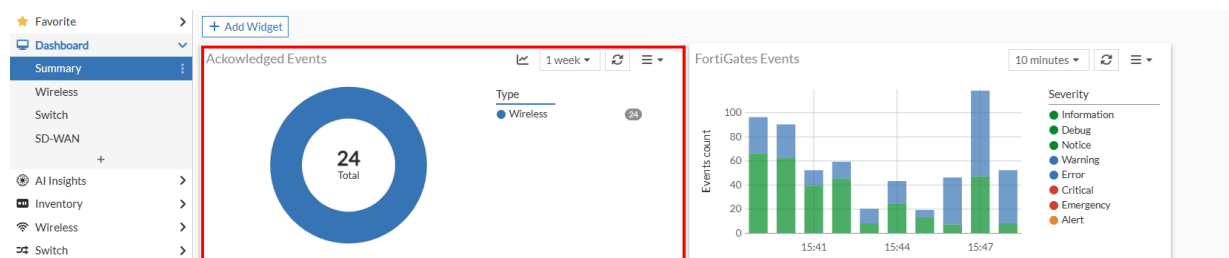
Summary

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

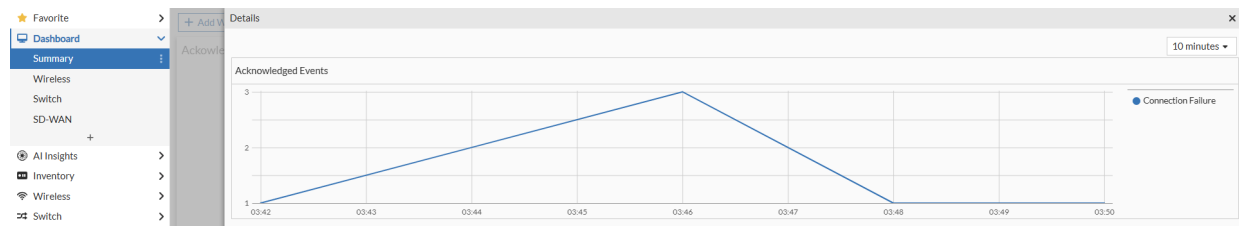


Acknowledged Events

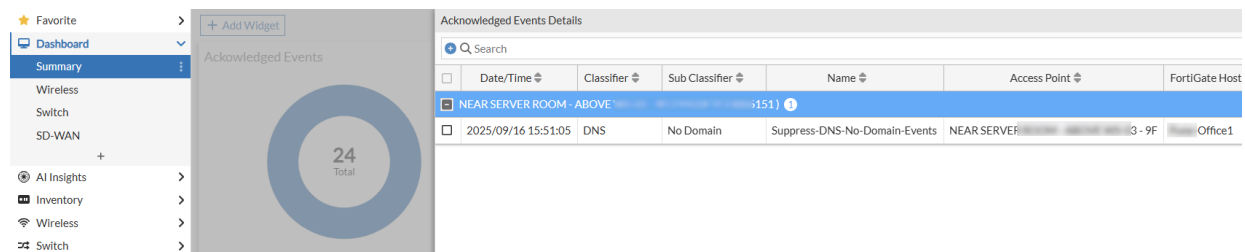
The **Acknowledged Events** chart offers a quick overview of acknowledged events. The chart shows the total number of acknowledged events and categorizes them by type within a specific timeframe.



Click the  icon to see a line chart that breaks down the number of acknowledged events over a period for a specific SLA.



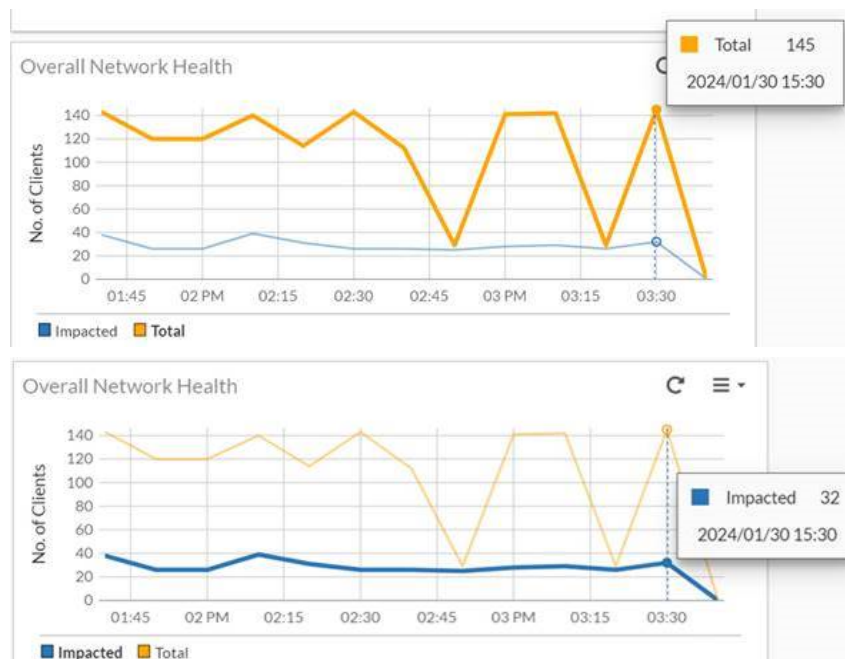
Click the chart itself to open the **Acknowledged Events Details** pane, which provides more in-depth information.



Overall Network Health

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

Hover over the  line to view the total number of clients and the  line to view the number of impacted clients. In this example, at 03:30 hours, a total of 145 clients were present in the network of which 32 clients are impacted.



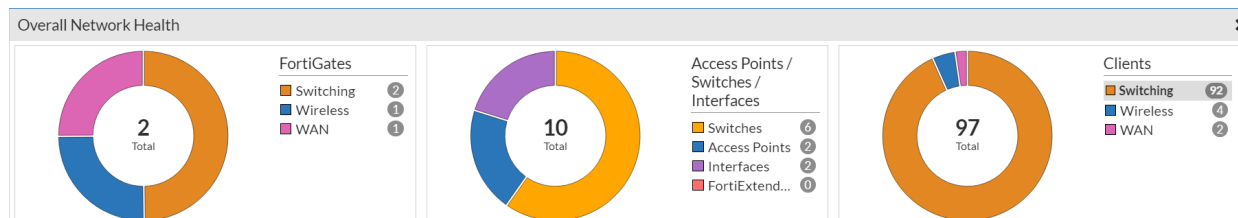
Click on any given time interval for total clients to view the **Connected Clients** panel. The data displayed in tabular format in all the monitor dashboard pages is filterable based on columns, you can group data by a specific column or filter data for specific values.

Connected Clients					
Wireless Switching					
Search					
MAC Address	FortiGate	IP Address	AP Name	SSID	Device
			FP221	simulator2.4G	
			FP221	simulator2.4G	
			FP221	simulator2.4G	

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

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

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



Switching Clients

Search filterable columns						
Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	FortiSwitch Name	FortiSwitch Serial Number	Con
2FLB2 71						
Switch Health and Uptime	10:40:30-10:40:30	FGT3K00P17N01177	10.33.4.130	10:40:30-10:40:30	10:40:30-10:40:30	10
Switch Health and Uptime	10:40:30-10:40:30	FGT3K00P17N01177	10.33.4.130	2FLB2	10:40:30-10:40:30	10

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

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

Click on the impacted SLA to view the device topology.

Top 5 Problematic Devices

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

Top 5 Problematic Devices	
🗕 1248E7F1 20012866	Impacted Clients: 37
🗕 2FLB2	Impacted Clients: 35
🗕 5424CF38 13000076	Impacted Clients: 20
🗕 5424E7F1 22001486	Impacted Clients: 16
🗕 1 SuperCheck_233F	Impacted Clients: 12

Click on the device name to view details.

Problematic device

FortiSwitch Serial Number == S248E7F1 20012866

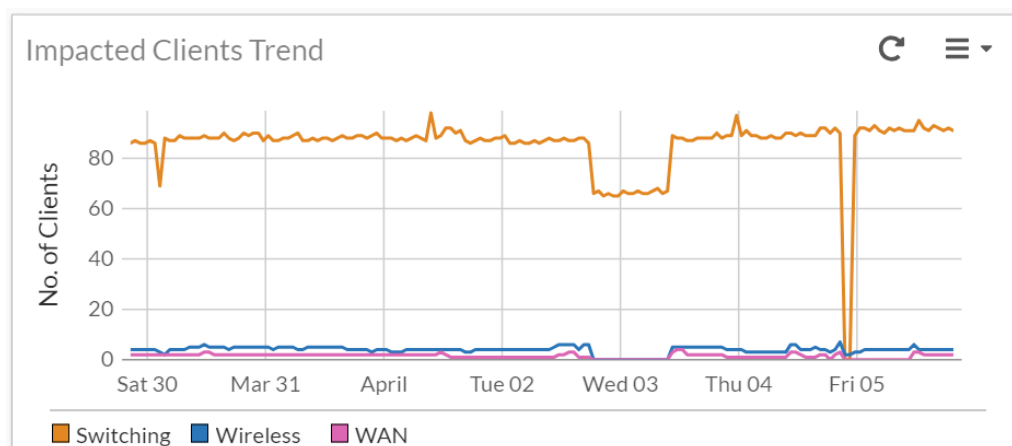
FortiGate Serial Number == FGT1K03D0P17N01177

Search filterable columns

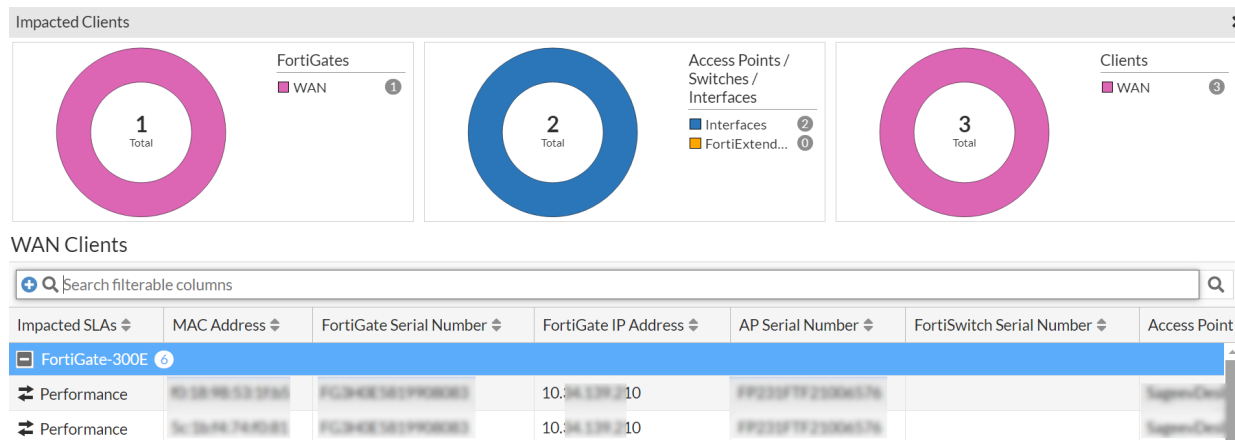
Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	FortiSwitch Name	FortiSwitch Serial Number
2FLB2 37/93					
Switch Health and Uptime	0016:2F:4C:76:26	FGT1K03D0P17N01177	10.33.4.130	1248E7F1 20012866	1248E7F1 20012866
Switch Health and Uptime	0016:2F:37:66:56	FGT1K03D0P17N01177	10.33.4.130	1248E7F1 20012866	1248E7F1 20012866
Switch Health and Uptime	52:53:66:C2:64:08	FGT1K03D0P17N01177	10.33.4.130	1248E7F1 20012866	1248E7F1 20012866

Impacted Clients Trend

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



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



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

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

FortiGates

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

FortiGate Events

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

Event Details							
Level = notice × + Q Search Q							
Timestamp	Level	Action	Message	SSID	Station MAC Address	Log ID	Fortigate Serialnumber

FortiGates CPU Usage and FortiGates Memory Usage

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

FortiGate CPU Usage							
CPU Usage = 0 -> 29 + Q Search							
Timestamp	FortiGate Name	Firmware Version	Model	Online APs	Offline APs	Clients	
2023/04/05 13:15:46		v7.2.3	FGVM64	1	14	0	
2023/04/05 13:15:49		v7.2.4	FG3H0E	7	10	3	8.

FortiGate Memory Usage							
Memory Usage = 30 -> 59 + Q Search							
Timestamp	FortiGate Name	Firmware Version	Model	Online APs	Offline APs	Clients	Throughput

High Latency FortiGates

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

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

High Latency FortiGates				
View stats + Q Search filterable columns				
Date/Time	Hostname	FortiGate IP Address	FortiGate Timeout	Failed API Count
2024/04/03 00:51:54	FortiGate-60E	10.17.24.11	3000	1
2024/04/03 02:22:21		10.17.44.9	3000	4
2024/04/03 02:31:54	HA-Primary	10.16.139.225	3000	7

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

Failed API details	
+ Q Search filterable columns	
Date/Time	API Endpoint
2024/04/03 01:11:54	/api/v2/monitor/traffic/.../select?count=5000
2024/04/03 01:21:54	/api/v2/monitor/traffic/.../select?count=5000
2024/04/03 01:51:54	/api/v2/monitor/traffic/.../select?count=5000

Wireless

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

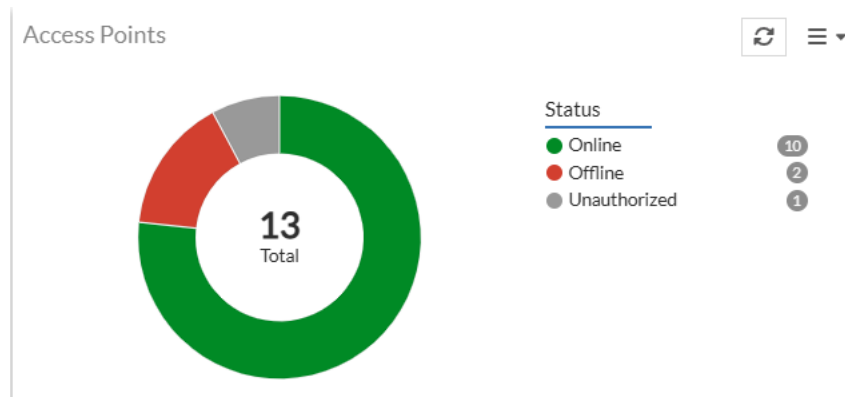
The following charts are available in the **Wireless** page:

- [Access Points](#)
- [WIDS Events](#)

- [Access Points CPU Usage](#)
- [Access Points Memory Usage](#)
- [Wireless](#)
- [Top 3 Impacted Apps](#)
- [Wireless Insights](#)
- [Rogue APs](#)
- [Applications by Usage](#)
- [Client Capability](#)

Access Points

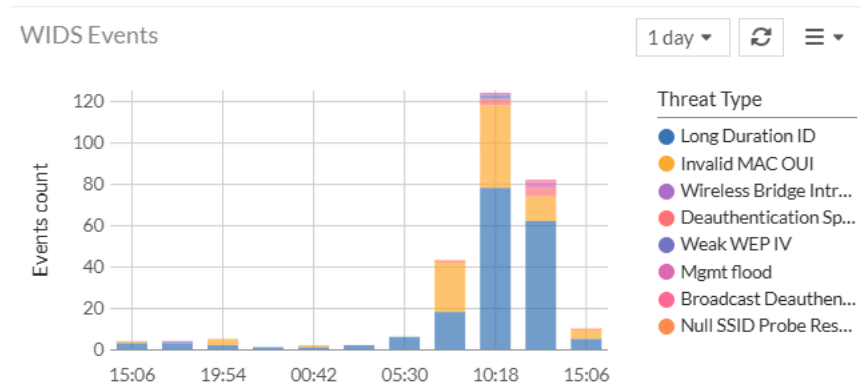
This chart displays the total number of access points in your network and their status (Online, Offline, Waiting for Authorization, or Unknown).



Click the chart for detailed information about the Access Points in use. For more information, see [Access Points](#).

WIDS Events

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



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

WIDS Events

Threat Type == Long Duration ID

Search filterable columns

Details

	Date/Time	Level	Action	Message	SSID	Station MAC Address	Log ID	FortiGate Serial
☐	2025/06/09 12:40:37	■■■■■■■■	wids-detect-first	WIDS long_dur: rts/NO from ea:57:af:30:85:56 chan 64...			0104043534	FG3
☐	2025/06/09 12:38:31	■■■■■■■■	wids-detect-first	WIDS long_dur: rts/NO from 96:5d:c6:52:fc:14 chan 36 d...			0104043534	FG3
☐	2025/06/09 12:36:07	■■■■■■■■	wids-detect-first	WIDS long_dur: rts/NO from 0a:0e:76:62:1d:64 chan 15...			0104043534	FG3

Double-click on an event to view more details

General

Absolute Date/Time

2025/06/09 12:40:37

Time

12:40:37

Virtual Domain

root

Log Description

Wireless long duration attack detected

Source

MAC Address

N/A

Interface

N/A

SSID

N/A

User

N/A

Action

Action

wids-detect-first

Reason

N/A

Security

Level

■■■■■■■■

Security Mode

N/A

Encryption

N/A

Cellular

Serial Number

N/A

Event

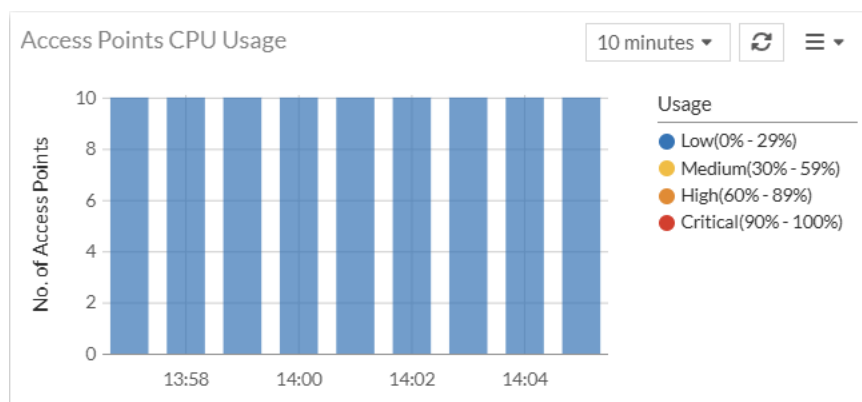
Serial Number

N/A

Close

Access Points CPU Usage

This chart displays the real-time FortiAP CPU usage at a given time and categorizes it as Low, Medium, High, and Critical. You can select the period to view the resource usage (10 or 30 minutes, 1 or 12 hours, or 1 day).

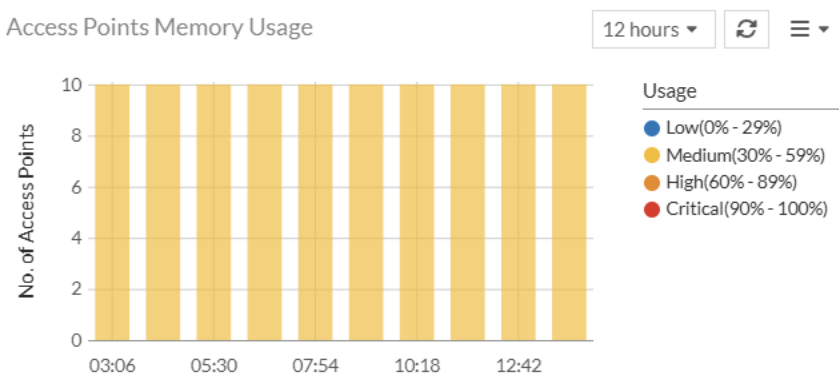


Click on the CPU usage chart to view more details.

Access points Health									
CPU Usage = 0 -> 29									
	Date/Time	FortiGate Name	AP Name	Memory Usage	CPU Usage	Temperature 1	Temperature 2	Temperature 3	VDOM
☐	2025/06/06 14:05:23	office	(00) FAP43...	58%	6%	46	47	45	root
☐	2025/06/06 14:05:23	office	(00) 6.83x...	41%	11%	48	48	47	root
☐	2025/06/06 14:05:23	office	(00) 1.83x...	42%	11%	44	44	44	root
☐	2025/06/06 14:05:23	office	(00) 8.83x...	41%	10%	48	48	48	root
☐	2025/06/06 14:05:23	office	(00) 2.FAP...	40%	9%	49	50	49	root
☐	2025/06/06 14:05:23	office	(00) 7.83x...	41%	6%	51	50	49	root
☐	2025/06/06 14:05:23	office	(00) 9.83x...	41%	9%	45	46	45	root
☐	2025/06/06 14:05:23	office	(00) 4.83x...	41%	10%	48	48	48	root
☐	2025/06/06 14:05:23	office	(00) 8.3x...	39%	9%	45	45	44	root
☐	2025/06/06 14:05:23	office	(00) 3.83x...	41%	11%	51	51	50	root

Access Points Memory Usage

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



Click on the memory chart to view more details.

Access points Health

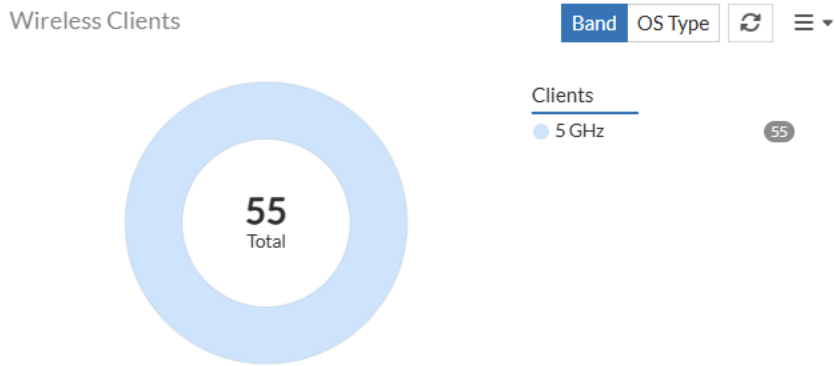
Memory Usage = 30 -> 59

Search filterable columns

	Date/Time	FortiGate Name	AP Name	Memory Usage	CPU Usage	Temperature 1	Temperature 2	Temperature 3	VDOM
☐	2025/06/06 05:25:11	office	9.833	40%	8%	52	52	51	root
☐	2025/06/06 05:24:10	office	3.833	40%	11%	53	54	52	root
☐	2025/06/06 05:21:11	office	2.FA	40%	10%	55	55	54	root
☐	2025/06/06 05:05:11	office	8.833	40%	9%	52	53	52	root
☐	2025/06/06 05:00:11	office	4.833	40%	12%	53	52	52	root
☐	2025/06/06 04:51:11	office	7.833	40%	6%	54	54	53	root
☐	2025/06/06 04:49:11	office	1.833	41%	11%	54	54	54	root
☐	2025/06/06 04:42:10	office	FAP	56%	6%	49	49	47	root
☐	2025/06/06 04:34:11	office	6.833	40%	9%	53	53	51	root
☐	2025/06/06 04:21:11	office	83X	39%	10%	58	58	57	root

Wireless Clients

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



Click on the chart to view more details. For more information, see [Wireless Clients](#).

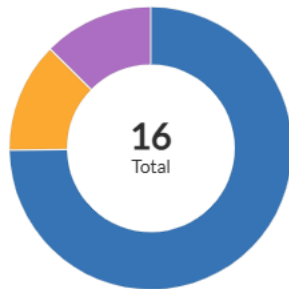
Top 3 Impacted Apps

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

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

Top 3 Impacted Apps

1 week



Apps

- MS Teams
- WhatsApp
- Zoom

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

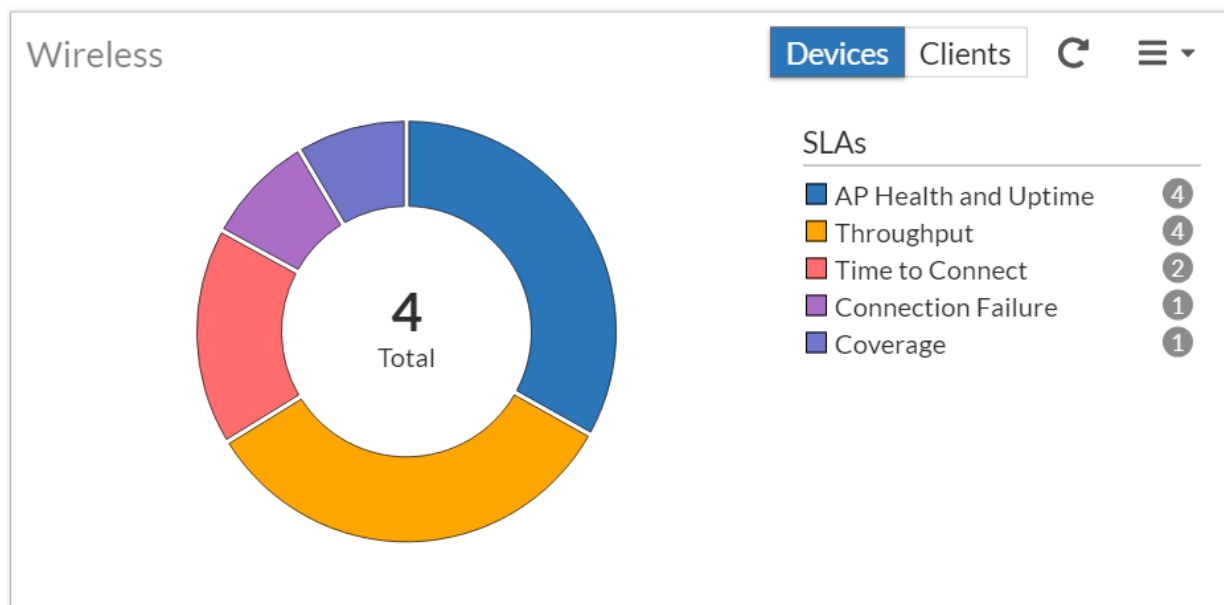
Top impacted apps									
View details Appname == Zoom Search filterable columns									
	Hostname	MAC Address	Timestamp	Downtime	Username	AP Serial Number	Sessions	Bandwidth Tx	Bandwidth Rx
☐	IND	04:cf	2025/06/03 11:36:21	1m		FP83	1	1.73 kB/s	15.99 kB/s
☐	IND	bc:03	2025/06/03 11:36:21	1m		FP83	1	6.1 kB/s	13.07 kB/s

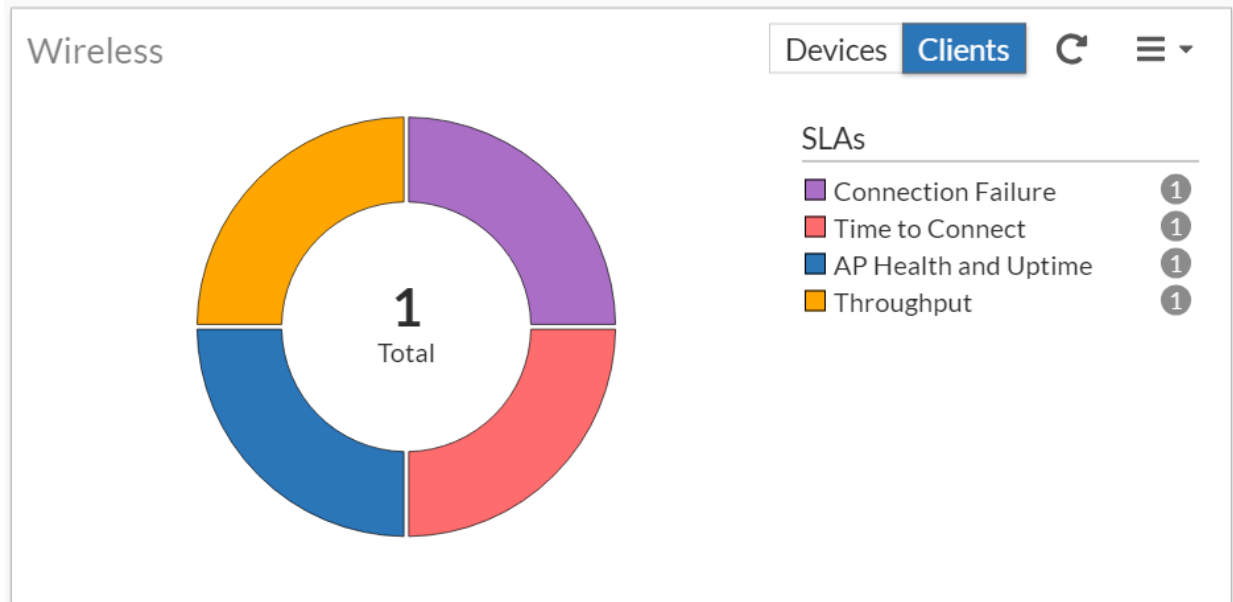
The applications are classified as impacted based on the downtime it experiences during various sessions in the selected time period. You can view the downtime for the latest session and the number of sessions. Furthermore, click on the number of sessions to view the downtime and other details for each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

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

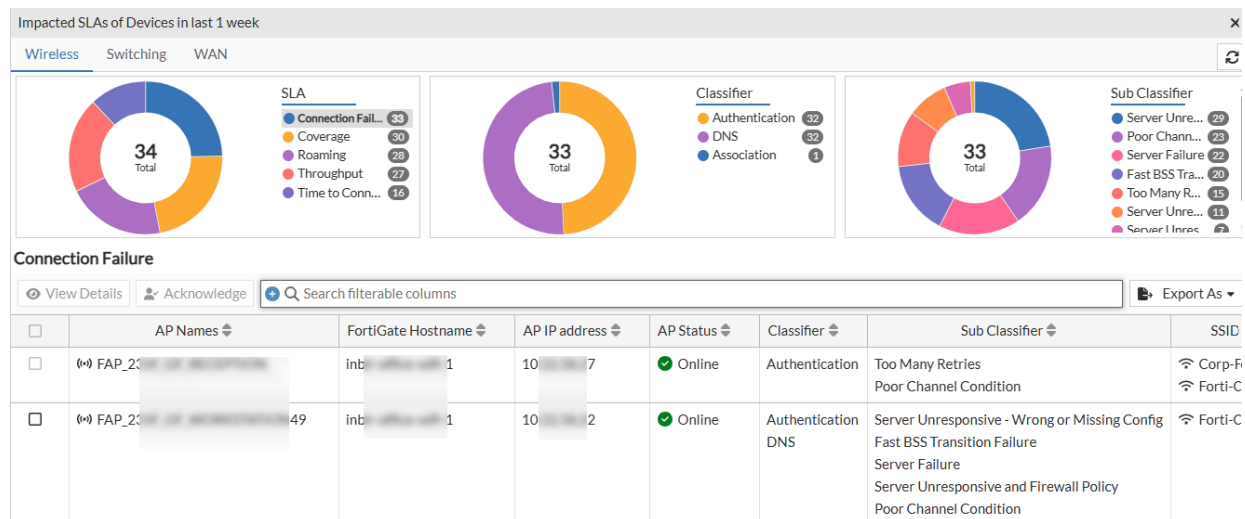
Wireless Insights

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

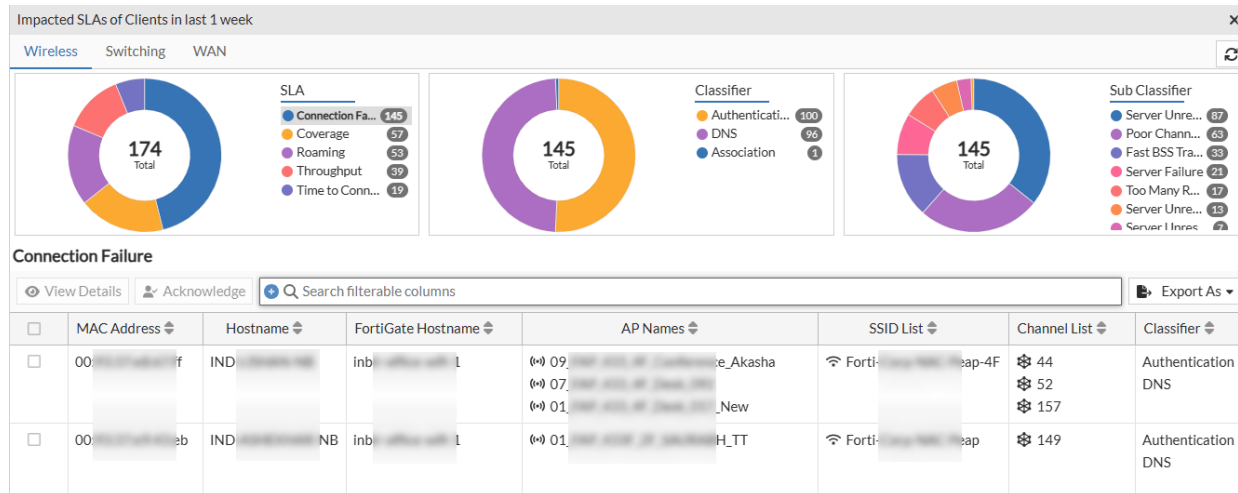




The impacted SLAs are detected and reported by FortiAI Ops with device and client details. The issues reported are categorized based on classifiers and sub-classifiers, with suggested remedial measures to curtail the SLA breaches and enhance network performance. The data displayed in this panel is for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



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

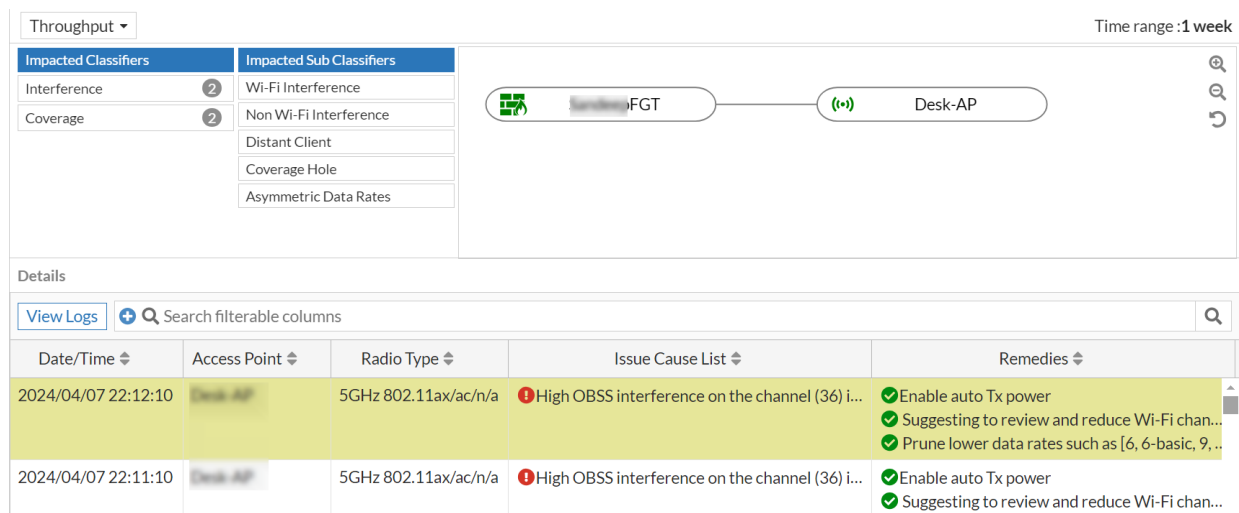


Select any row and click **View Details** to view a simplified topology with a visualization/illustration of the physical placement of devices, such as, FortiGate, FortiSwitch, and FortiAPs connected to each other in your network. This hierarchical pattern is representational; you cannot modify the placement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

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

Throughput

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



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

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

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

Throughput Logs

Diagnostics

AP Stats

AP Logs

Switch Info

Neighbour APs

WIFI Clients

Interfering APs

AP Info

Name	PU431F5E19001086
Serial	PU431F5E19001086
Mac Address	00-0c-a6-7c-d7-b0
IP Address	192.168.100.16
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 - 85240F5C18000043 (port17)
Remedy	Suggesting to configure Auto negotiation for switch port(s) and also to review if switch port supports full duplex

Close

Logs**Description****Diagnostics**

This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAI Ops 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

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								
☐	Date/Time ⌵	Radio Type ⌵	Bandwidth Tx ⌵	Bandwidth Rx ⌵	Channel Utilization(%) ⌵	Client Count ⌵	Oper Chan ⌵	Oper Tx Power ⌵
☐	2025/06/23 12:37:23	802.11ax-5G	3.03 Mbps	1.43 Mbps	48	337	100	26 dBm

AP Logs

This tab provides the AP event logs generated from FortiGate.

Logs

Description

Date/Time	AP Name	Action	Message	Log Desc
2023/11/09 12:35:48.871	43x_2F_CS_Bay	client-disconnected-by-wtp	Client 04:cf:4b:b3:3d:19 disconnected b...	Wireless client WTP disc
2023/11/09 12:38:29.019	43x_2F_CS_Bay	auth-req	AP received authentication request fra...	Authentication request f
2023/11/09 12:38:29.019	43x_2F_CS_Bay	auth-resp	AP sent authentication response frame t...	Authentication response
2023/11/09 12:38:29.019	43x_2F_CS_Bay	reassoc-req	AP received reassociation request frame...	Reassociation request fr
2023/11/09 12:38:29.019	43x_2F_CS_Bay	reassoc-resp	AP sent reassociation response frame to...	Reassociation response t

Switch Info

This tab displays the configuration details of the switch port connected to the AP.

Switch Config							
+ Search							
Switch Name	Interface	Duplex	Speed	Status	Collisions	Rx Bytes	Tx bytes
Switch1	port15	full	1000	up	0	840629319	5317837210

Neighbour APs

This tab displays details of the detected neighbour APs by the client, for distant client & coverage hole issues.

+ Search			
AP Radio	Band	RSSI	RSSI Age
FP231F	5 GHz	18	37
FP431F	5 GHz	22	38
FP431F	5 GHz	16	38

WIFI Clients

This tab provides details of the impacted clients and also lists all the clients associated with the AP.

Date/Time	Client Mac Address	SSID	Radio Type	Classifier	Subclassifier	Signal Strength
2022/05/24 13:23:42	8a:2b:2c:3d:4e:5f	Forti-Client	802.11ax-5G	Coverage	Asymmetric Data Rates	-54 dBm
2022/05/24 13:23:42	8a:2b:2c:3d:4e:5f	Forti-Client	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	8a:2b:2c:3d:4e:5f	Forti-Client	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	8a:2b:2c:3d:4e:5f	Forti-Client	802.11ac	Coverage	Asymmetric Data Rates	-54 dBm

0% 5

All Clients						
+ Search						
Client Mac Address	Channel	Radio Type	SSID	Data Rate	Bandwidth Rx	Bandwidth Tx
8a:2b:2c:3d:4e:5f	60	802.11ax-5G	Forti-Client	456.00 Mbps	0	642.00 bps
8a:2b:2c:3d:4e:5f	60	802.11ax-5G	Forti-Client	12.00 Mbps	0	1.77 Kbps
8a:2b:2c:3d:4e:5f	60	802.11ax-5G	Forti-Client	797.20 Mbps	426.39 Kbps	45.10 Kbps

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	XXXXXXXXXX	-67 dBm
2023/11/07 16:23:26	XXXXXXXXXX	-67 dBm
2023/11/07 16:23:26	XXXXXXXXXX	-67 dBm
2023/11/07 16:23:26	XXXXXXXXXX	-82 dBm

Connection Failure

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

Connection Failure ▾

Time range :1 week

Impacted Classifiers	Impacted Sub Classifiers
Association ①	DHCP NAK
Authentication ①	Too Many Retries
DNS ①	Poor Channel Condition
	No Domain
	Server Failure

Details

View Logs

Search filterable columns

Date/Time ↕	MAC Address ↕	Hostname ↕	Issue Cause List ↕	Remedies ↕
2024/04/07 18:23:49	88:45:a2:42:46:93	DESKTOP-138787D	❗ Wireless station DNS process failed due to n...	✅ Check local domain name(s) configured for t...
2024/04/07 14:27:06	88:45:a2:42:46:93	DESKTOP-138787D	❗ Wireless station DNS process failed due to n...	✅ Check local domain name(s) configured for t...
2024/04/07 14:26:04	88:45:a2:42:46:93	DESKTOP-138787D	❗ Wireless station DNS process failed due to n...	✅ Check local domain name(s) configured for t...

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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
Access Point	The name of the AP that the impacted client associated with.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Issue Cause List	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.

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

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

Client Details

Association Time

2023-11-08 10:53:57

Channel

116

FortiAP

MIMO

2x2

SSID

Forti-XXXXXX

5GHz

Band

-72dBm

Signal Strength

20dB

Signal Strength/Noise

0%

Transmission Discard

2%

Transmission Retry

CLIENT LOGS

+

Q Search

Q

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

0% 22

Time to Connect

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

Time to Connect ▾
Time range :1 week

Impacted Classifiers	Impacted Sub Classifiers
Authentication Delay 1	Coverage or Load Issue
DHCP Delay 1	Poor Bandwidth

Details

View Logs + Search filterable columns

Date/Time ▾	MAC Address ▾	Hostname ▾	Issue Cause List ▾	Remedies ▾
2024/04/05 18:15:39	94-40-40-35-40-40		! AP health - detected high channel utilization. ...	✓ Rectify the channel utilization issue. Alternati...
2024/04/04 19:51:04	94-40-40-35-40-40		! Wired Network - packet delays detected	✓ Check switch side connections and configurat...
2024/04/04 16:32:03	94-40-40-35-40-40		! Wired Network - packet delays detected	✓ Check switch side connections and configurat...

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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Signal Strength	The signal strength of the client at the time of impact.
Issue Cause List	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies to resolve the issue.
Access Point	The name of the access point that the client associated with.
AP Serial Number	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
User Name	The impacted client user name.
Association Delay	The association delay measured in milliseconds.
Association Time	The total time taken by the client for association.
Authentication Delay	The authentication delay measured in milliseconds.

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

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

Client Details

Association Time	2023-11-08 10:53:57	5GHz	Band
Channel	116	-72dBm	Signal Strength
FortiAP		20dB	Signal Strength/Noise
MIMO	2x2	0%	Transmission Discard
SSID	Forti-XXXXXX	2%	Transmission Retry

CLIENT LOGS

Search

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

0% 22

Coverage

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

Coverage ▾

Time range : 1 week

Impacted Classifiers

Coverage hole 2

Overlapping APs 2

Impacted Sub Classifiers

Poor Coverage

No better neighbour AP f...

Wi-Fi Interference

Details

View Logs

Search filterable columns

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

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

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

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

Coverage Logs

[Diagnostics](#)
[AP Stats](#)
[AP Logs](#)
[Neighbour APs](#)
[WiFi Clients](#)
[Interfering APs](#)

AP Info

Name	43x_2F_...
Serial	...
Mac Address	...
IP Address	...
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

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

FortiAIOps 3.2.1 User Guide
Fortinet Inc.

101

Logs

Description

AP Logs

This tab provides the AP event logs generated from FortiGate.

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

WIFI Clients

This tab provides details of the impacted clients and also lists all the clients associated with the AP.

Date/Time	Client Mac Address	SSID	Radio Type	Classifier	Subclassifier	Signal Strength
2022/05/24 13:23:42	88:00:00:00:00:00	Forti-Client-K	802.11ax-5G	Coverage	Asymmetric Data Rates	-54 dBm
2022/05/24 13:23:42	88:00:00:00:00:00	Forti-Client-K	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	88:00:00:00:00:00	Forti-Client-K	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	88:00:00:00:00:00	Forti-Client-K	802.11ac	Coverage	Asymmetric Data Rates	-54 dBm

0% 5

All Clients

 Search

Client Mac Address	Channel	Radio Type	SSID	Data Rate	Bandwidth Rx	Bandwidth Tx	
88:00:00:00:00:00	60	802.11ax-5G	Forti-Client-K	456.00 Mbps	0	642.00 bps	
88:00:00:00:00:00	60	802.11ax-5G	Forti-Client-K	12.00 Mbps	0	1.77 Kbps	
88:00:00:00:00:00	60	802.11ax-5G	Forti-Client-K	797.20 Mbps	426.39 Kbps	45.10 Kbps	

Interfering APs

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

Date/Time	BSSID	Signal Strength
2023/11/09 13:25:09	88:00:00:00:00:00	-73 dBm
2023/11/09 13:25:09	88:00:00:00:00:00	-46 dBm
2023/11/09 13:25:09	88:00:00:00:00:00	-47 dBm

Roaming

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

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

Attribute

Description

Date/Time

The date and time of the impact as per your timezone.

MAC Address

The MAC address of the impacted client device.

Device

The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.

SSID

The SSID that the impacted client is associated with.

Classifier

The classifier of the issue reported for the SLA.

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

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

Client Details	
Diagnostics AP Stats Client Logs	
Issue Diagnostics	
Issue Cause	Roaming delay observed for 11r roaming over-the-ds
Remedy	Review threshold computed/configured for 11r Roaming delay alerts.

Logs

Diagnostics

This tab provides detailed cause of the SLA breach that impacted the client. FortiAI Ops also suggests the remedy to resolve the issue.

Issue Diagnostics

Issue Cause

Roaming delay observed for 11r roaming over-the-air

Remedy

Review threshold computed/configured for 11r Roaming delay alerts.

AP Stats

This tab displays the details of the AP radio that the client associated with.

Radio Info

Search

Radio Type

802.11ax-5G

Bandwidth Tx

209.92 Kbps

Bandwidth Rx

158.65 Kbps

Channel Utilization(%)

31

Client Count

15

Oper Chan

60

Oper Tx Power

10 dBm

Client Logs

This tab provides client event logs.

Logs

Description

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

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

AP Health and Uptime

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

AP Health and Uptime
Time range : 1 week

Impacted Classifiers	Impacted Sub Classifiers
AP Down 1	FGT Shutdown
CPU 1	FGT Reboot
Memory 1	FSW Port Down
Switch Health 1	Poor Uplink Connectivity
	FAP Reboot
	Configuration Issue or Ot...
	High Resource Utilization

Details

View Logs
Search filterable columns

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

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

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

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

AP Details

Diagnostics
AP Stats
Logs
WIFI Clients
Interfering APs

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.

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

Logs

- For the AP *down*/FortiSwitch health events, triggered due to FortiSwitch related failure, the FortiSwitch status and logs are displayed.
- For AP health related events like poor CPU and memory, the AP status and logs are displayed.
- For AP down events triggered due to FortiAP/FortiGate failure, the AP status and logs, and FortiGate logs are displayed.

SWITCH Status

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

SWITCH Logs

+ Search

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

FortiAIOps 3.2.1 User Guide
Fortinet Inc.

105

Logs	Description																																							
WIFI Clients	This tab provides details of the impacted clients and also lists all the clients associated with the AP. AP Details Impacted Clients <table border="1"> <thead> <tr> <th>Date/Time</th> <th>Client Mac Address</th> <th>Device</th> <th>AP Name</th> <th>Classifier</th> <th>Sub Classifier</th> </tr> </thead> <tbody> <tr> <td>2022/07/18 15:52:32</td> <td></td> <td>Corp</td> <td>AP</td> <td>Memory</td> <td>High Resource Utilization</td> </tr> <tr> <td>2022/07/18 15:52:32</td> <td></td> <td>Corp</td> <td>AP</td> <td>Memory</td> <td>High Resource Utilization</td> </tr> </tbody> </table> All Clients <table border="1"> <thead> <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> </tr> </thead> <tbody> <tr> <td></td> <td>6</td> <td>802.11n</td> <td>24ghz-25bridge</td> <td>136.00 Mbps</td> <td>0</td> <td>0</td> </tr> <tr> <td></td> <td>6</td> <td>802.11n</td> <td>24ghz-25bridge</td> <td>169.00 Mbps</td> <td>0</td> <td>0</td> </tr> </tbody> </table> OK Cancel	Date/Time	Client Mac Address	Device	AP Name	Classifier	Sub Classifier	2022/07/18 15:52:32		Corp	AP	Memory	High Resource Utilization	2022/07/18 15:52:32		Corp	AP	Memory	High Resource Utilization	Client Mac Address	Channel	Radio Type	SSID	Data Rate	Bandwidth Rx	Bandwidth Tx		6	802.11n	24ghz-25bridge	136.00 Mbps	0	0		6	802.11n	24ghz-25bridge	169.00 Mbps	0	0
Date/Time	Client Mac Address	Device	AP Name	Classifier	Sub Classifier																																			
2022/07/18 15:52:32		Corp	AP	Memory	High Resource Utilization																																			
2022/07/18 15:52:32		Corp	AP	Memory	High Resource Utilization																																			
Client Mac Address	Channel	Radio Type	SSID	Data Rate	Bandwidth Rx	Bandwidth Tx																																		
	6	802.11n	24ghz-25bridge	136.00 Mbps	0	0																																		
	6	802.11n	24ghz-25bridge	169.00 Mbps	0	0																																		
Interfering APs	This tab displays details of the interfering APs in your network. <table border="1"> <thead> <tr> <th>Date/Time</th> <th>BSSID</th> <th>Signal Strength</th> </tr> </thead> <tbody> <tr> <td>2023/11/07 16:23:26</td> <td></td> <td> -67 dBm</td> </tr> <tr> <td>2023/11/07 16:23:26</td> <td></td> <td> -67 dBm</td> </tr> <tr> <td>2023/11/07 16:23:26</td> <td></td> <td> -67 dBm</td> </tr> <tr> <td>2023/11/07 16:23:26</td> <td></td> <td> -82 dBm</td> </tr> </tbody> </table>	Date/Time	BSSID	Signal Strength	2023/11/07 16:23:26		-67 dBm	2023/11/07 16:23:26		-67 dBm	2023/11/07 16:23:26		-67 dBm	2023/11/07 16:23:26		-82 dBm																								
Date/Time	BSSID	Signal Strength																																						
2023/11/07 16:23:26		-67 dBm																																						
2023/11/07 16:23:26		-67 dBm																																						
2023/11/07 16:23:26		-67 dBm																																						
2023/11/07 16:23:26		-82 dBm																																						

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

AP Details

[Diagnostics](#)
[AP Stats](#)
[Logs](#)
[Interfering APs](#)

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.

Logs

Description

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

Q

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

Interfering APs

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

Date/Time	BSSID	Signal Strength
2023/11/07 16:23:26	80:00:00:00:00:00	-67 dBm
2023/11/07 16:23:26	80:00:00:00:00:00	-67 dBm
2023/11/07 16:23:26	80:00:00:00:00:00	-67 dBm
2023/11/07 16:23:26	80:00:00:00:00:00	-82 dBm

Logs

This tab provides the AP event logs generated from FortiGate.

WIDS

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

The following types of intrusion detection is available:

Intrusion Type	Description
Broadcast Deauthentication	This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
Long Duration ID	To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
Authentication Frame Flood	A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
Association Frame Flood	A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
Deauthentication Spoof	Spoofed de-authentication frames are a denial of service attack. They cause all clients to disconnect from the AP.
EAPOL Flood attacks	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be

Intrusion Type	Description
	a denial of service attack. Several types of EAPOL packets are detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, EAPOL-SUCC.
Wireless Bridge Intrusion	WiFi frames with both the fromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Invalid Mac OUI	Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
Weak WEP IV	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
ASLEAP Attack	ASLEAP is a tool used to perform attacks against LEAP authentication.

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

The screenshot displays the FortiGate WIDS (Wireless Intrusion Detection System) interface. On the left, a donut chart shows 5 total events. The main area features a topology diagram of a FortiGate-300E connected to several wireless clients. Below this, a table lists detected events with columns for Date/Time, Transmitter MAC, BSSID, Detected AP, Detected Radio ID, FortiGate Hostname, Classifier, and Sub Classifier.

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

11 Updated: 15:47:34

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

- Denial of Service
- Misconfigured Packet
- Rogue Attack

- Cipher Attack
- Tool Attack

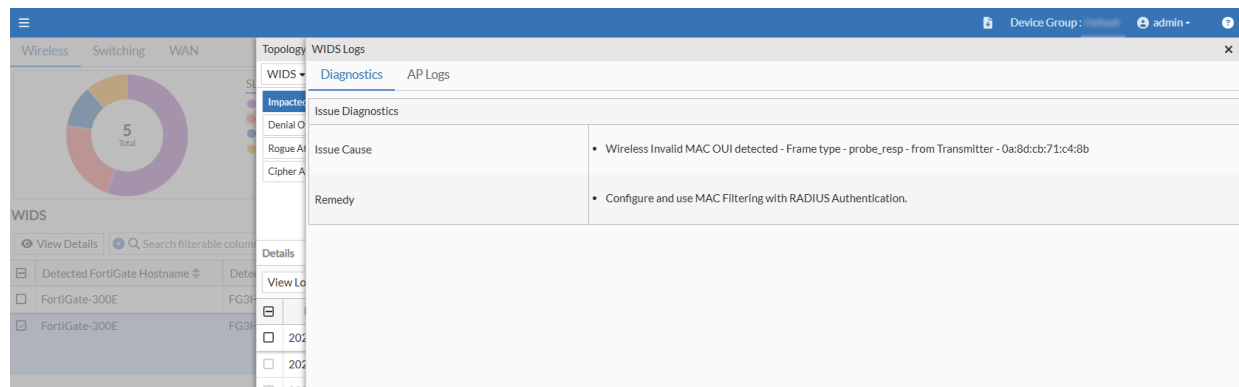
The **Details** table displays information such as the Detected FortiGate Hostname, Detected FortiGate, Affected AP Serial Number, Detected FortiGate IP Address, Classifier, Sub Classifier, Affected AP IP Address, Affected AP Name, Affected AP State, and Affected AP Status. Right-click on the header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

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

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

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

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



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

Topology WIDS Logs

WIDS Diagnostics AP Logs

Impacted

Denial O

Q Search

Q Details

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

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

WIDS Logs

Diagnostics AP Logs

Q Search

Q Details

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

General

Absolute Date/Time2025/04/25 14:17:37

Time14:17:38

Virtual Domainroot

Log DescriptionWireless long duration attack detected

Source

MAC AddressN/A

InterfaceN/A

SSIDN/A

UserN/A

Action

Actionwids-detect-first

ReasonN/A

Security

Level

Security ModeN/A

EncryptionN/A

Cellular

Serial NumberN/A

1

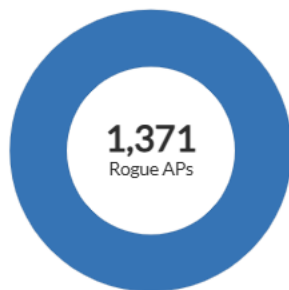
Close

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

Rogue APs

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

Rogue APs



Interfering FortiAPs

● Rogue APs

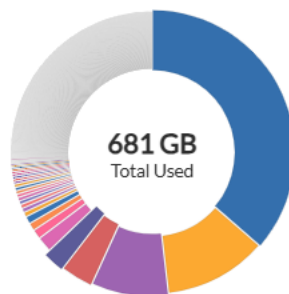
1,371

Click on the chart to view more details. For more information, see [Rogue APs](#).

Applications by Usage

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

Applications by usage



Apps

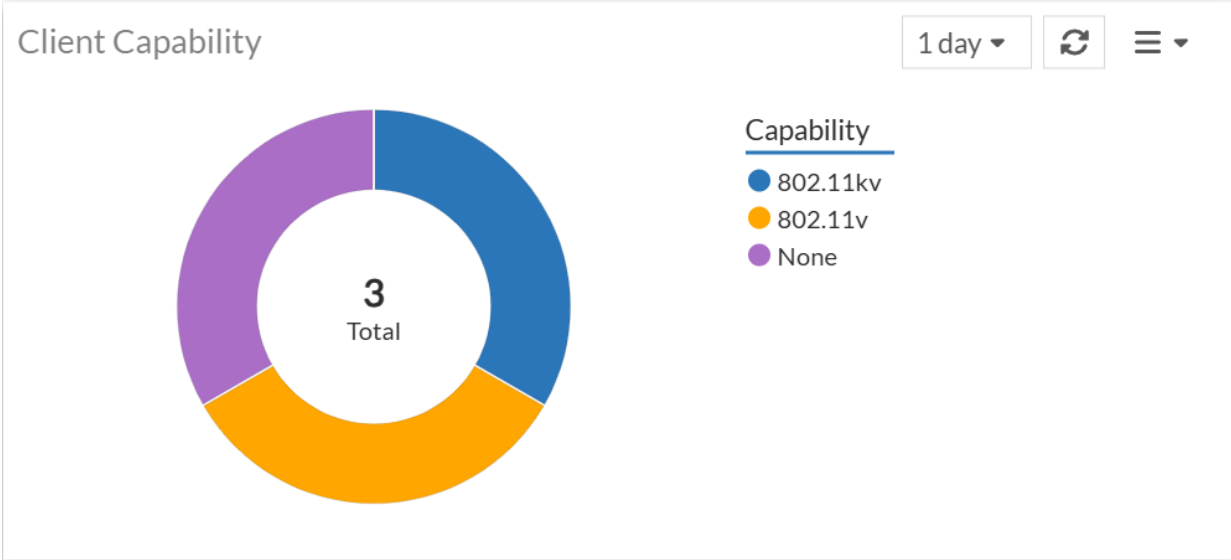
- DTLS
- FortiEDR.Core
- HTTPS.BROWSER
- SSL_TLSv1.3
- QUIC
- SSH
- RDP
- Microsoft.Teams
- Google.Services

Click on an application name to view more details. For more information, see [Applications](#).

Client Capability

The **Client Capability** widget provides a quick and informative overview of the connection health of wireless clients over a specific time period. The widget represents the total number of clients connected during that time, categorized by their connection status or capabilities.

To add the widget, navigate to **Dashboard > Wireless**. Click **Add Widget**.



- **Total:** The number in the center of the chart indicates the total number of clients that are connected during the specified time period.
- **Capability Legend:** The legend on the right explains what each colour segment of the chart represents. The categories are based on various Wi-Fi protocol standards and capabilities, which are often related to roaming and connection optimization.

Clicking on a specific category displays the **Station details** window with more details.

Stations details									
Q Search									
	MAC Address	AP Serialnumber	Channel	Bandwidth Tx/Rx	Signal St...	Signal Strength	Association Time	Technology	Device OS
☐	00:00:00:00:FA	FP8000000254	140	43.18 kbps	26 dB	-69 dBm	2025/09/15 14:37:45	802.11ax/ac/n/a	Windows
☐	08:00:00:00:8C	FP8000000277	44	38.77 kbps	44 dB	-51 dBm	2025/09/15 15:20:33	802.11ax/ac/n/a	Windows
☐	38:00:00:00:3F	FP8000000254	140	1.93 kbps	37 dB	-58 dBm	2025/09/15 01:01:14	802.11ax/ac/n/a	Ubuntu
☐	4C:00:00:00:19	FP8000000257	124	66 bps	59 dB	-36 dBm	2025/09/15 01:01:44	802.11ax/ac/n/a	Windows
☐	56:00:00:00:7A	FP8000000277	44	0 bps	32 dB	-63 dBm	2025/09/15 15:20:34	802.11ax/ac/n/a	Android
☐	60:00:00:00:93	FP8000000245	132	1.63 kbps	51 dB	-44 dBm	2025/09/15 01:01:14	802.11ax/ac/n/a	Windows
☐	7C:00:00:00:5A	FP8000000254	140	17.98 kbps	43 dB	-52 dBm	2025/09/15 15:34:16	802.11ax/ac/n/a	Windows
☐	A0:00:00:00:DE	FP8000000277	44	93.88 kbps	61 dB	-34 dBm	2025/09/15 12:33:24	802.11ax/ac/n/a	Windows
☐	BC:00:00:00:CA	FP8000000277	44	63.52 kbps	50 dB	-45 dBm	2025/09/15 15:27:58	802.11ax/ac/n/a	Windows

The search bar and sorting options for each column allows a network administrator to quickly find and analyze specific station details.

Switch

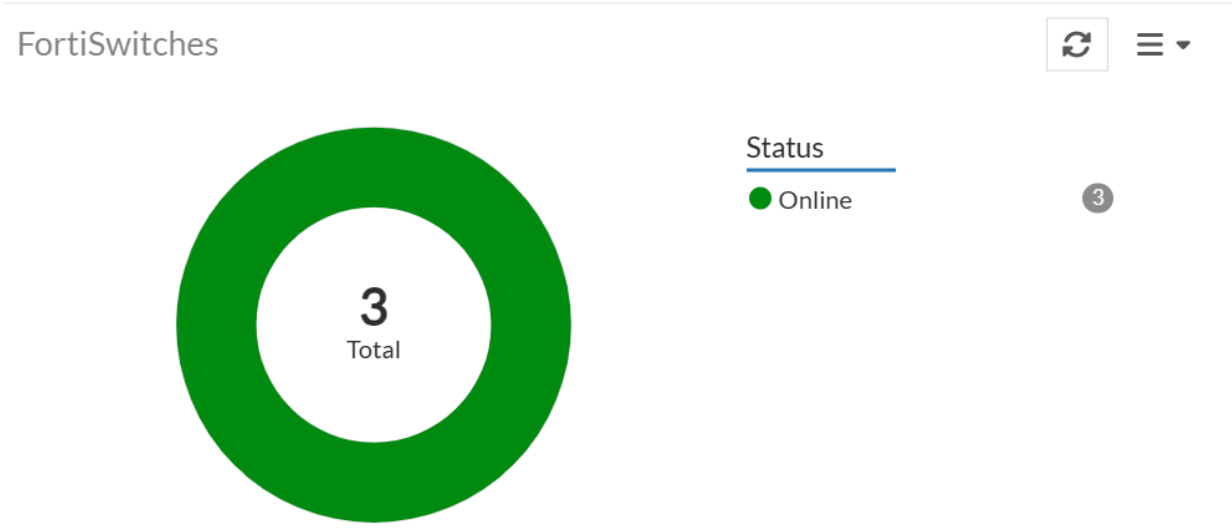
The Switch page displays all the important details about the switches within your network. Details of all the FortiSwitches and their status, the types of even in a specific time period, details of the wired clients, and different SLAs displayed.

The following charts are available:

- [FortiSwitches](#)
- [FortiSwitches Events](#)
- [Wired Clients](#)
- [Switching Insights](#)

FortiSwitches

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



Click the chart for detailed information about the FortiSwitches.

FortiSwitches

3
Total

Status

● Online

3

3
Total

Model

● FortiSwitch S224D...

● FortiSwitch S248D...

● FortiSwitch S548D...

View details

CLI

Search filterable columns

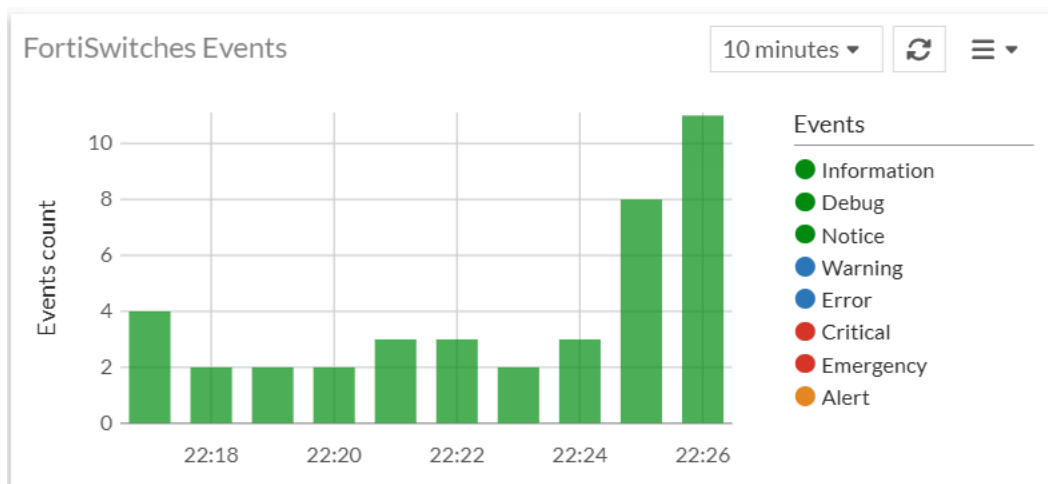
Export As

	Name	FortiSwitch Serial Number	FortiGate	Status	Model	Firmware Version	Connecting From	Join Time
☐	3FH	S224	office	Online	S224DF	S224DF-v7.6.1-build1047,241217 (GA)	10.	2025/06/05 17:53:48
☐	GFF	S248	office	Online	S248DF	S248DF-v3.6.12-build436,230614 (GA)	10.	2025/06/05 17:51:58
☐	2FS	S548	office	Online	S548DF	S548DF-v7.4.0-build767,230602 (GA)	10.	2025/06/05 17:51:53

For more information, see [FortiSwitch](#).

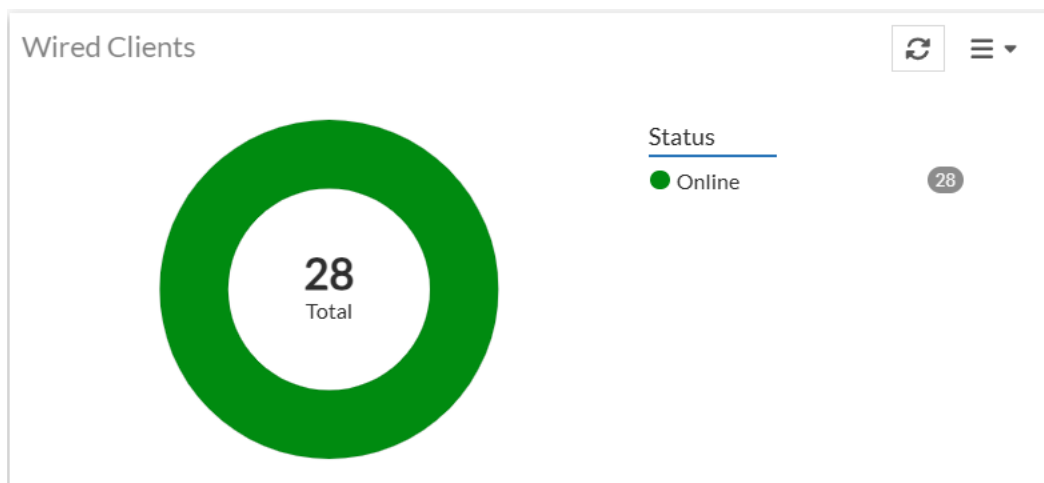
FortiSwitches Events

This chart displays the FortiSwitch events at a given time and categorizes them based on the type of event as Information, Debug, Notice, Warning, Error, Critical, Emergency, and Alert. You can select the period to view the data (10 or 30 minutes, 1 or 12 hours, or 1 day).



Wired Clients

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



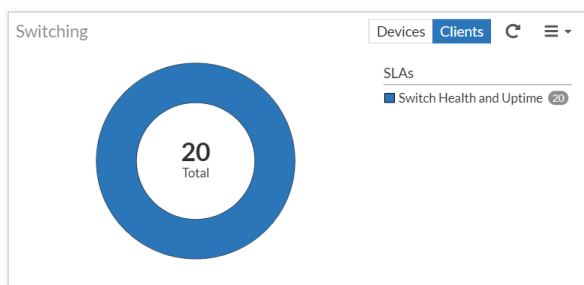
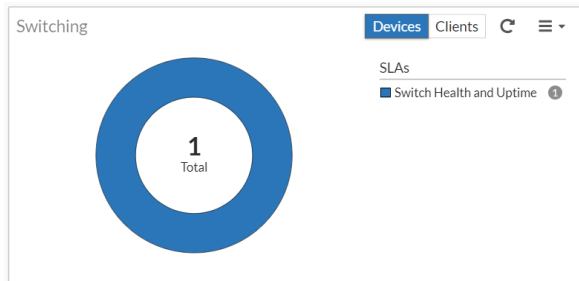
Click on the chart to view more details. For more information, see [Wired Clients](#).

Switching Insights

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

Notes:

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



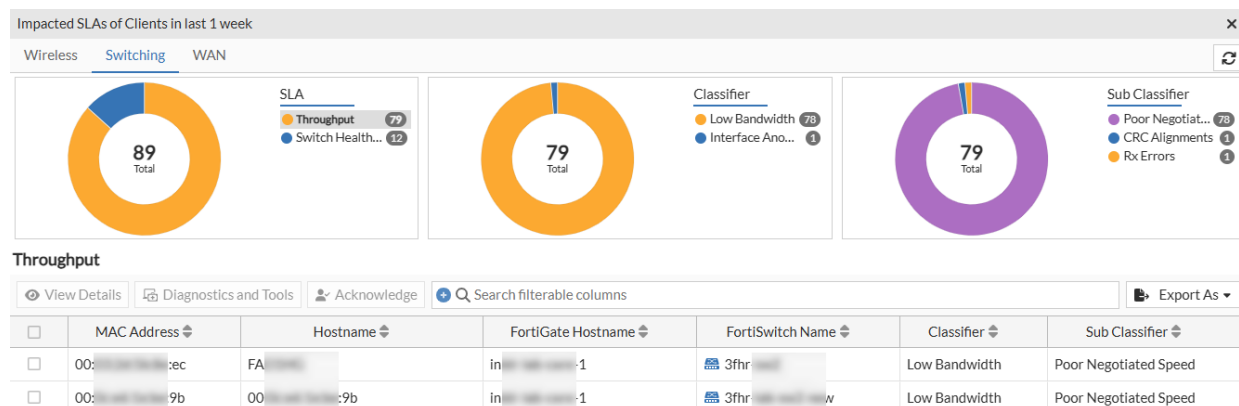
SLAs, Topology and Logs

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

- [Throughput](#)
- [Network](#)
- [Switch Health and Uptime](#)
- [Switch](#)

Throughput

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



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

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

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

Topology of 50:3e:aa:b1:70:34

Throughput Time range: 1 week

Impacted Classifiers

Congestion 1

Low Bandwidth 1

Impacted Sub Classifiers

Tx Congestion

Details

View Logs Search filterable columns

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

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

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

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

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

Switch Logs ×

[Diagnostics](#)
[Switch Statistics](#)

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

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

Close

Switch Logs

DiagnosticsSwitch Statistics

Port Status

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

Port Statistics

Search filterable columns

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

Network

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

Impacted SLAs of Clients in last 1 week

WirelessSwitchingWAN

21
Total

SLA

- Switch Health... 20
- Throughput 16
- Network 3
- Switch Connec... 1

3
Total

Classifier

- STP 3
- Storm 1

3
Total

Sub Classifier

- Interface Do... 3
- BPDU Loss 3
- Loop Detect 3
- Role Transiti... 2
- Superior BP... 2
- Broadcast ST... 1
- Multicast Str... 1

Network

View DetailsDiagnostics and ToolsAcknowledge

Search filterable columns

Export As

☐	MAC Address	Hostname	FortiGate Hostname	FortiSwitch Name	Classifier	Sub Classifier
☐	00:00:00:00:00:00a4	PU3:00:00:00:00:00DILV	G1K:00:00:00:00:00S_SIM	S5:00:00:00:00:00551	STP	Interface Down BPDU Loss Role Transition Blocked Loop Detect
☐	00:00:00:00:00:00a7	MAC:00:00:00:00:008666	G1K:00:00:00:00:00S_SIM	S5:00:00:00:00:00551	STP	Interface Down BPDU Loss Superior BPDU Loop Detect

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

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

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

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

Network
Time range: 2 hours

Impacted Classifiers
Impacted Sub Classifiers

Storm 1
Broadcast Storm
Multicast Storm

FortiGate-300E-sa...
S524DF4K...

Details

View Logs
Search

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

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

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

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

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

Switch Logs ×

[Diagnostics](#)
[Switch Statistics](#)

Switch Info

FortiGate Hostname	FortiGate-300E-3
FortiGate Serial No	FG3H0E5
IP Address	10.34.
Switch Name	S524DF4K
Switch Serial	S524DF4K
Status	Connected
State	Authorized
Version	S524DF-v7.4.3-build830,240422 (GA)
Connecting From	169.

Issue Diagnostics

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

Close

Switch Logs

Diagnostics

Switch Statistics

Port Status

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

Port Statistics

Search filterable columns

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

Switch Health and Uptime

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

Impacted SLAs of Devices in last 1 week

Wireless

Switching

WAN

7

Total

SLA

Switch Health an...

Throughput

6

Total

Classifier

Port Down

6

Total

Sub Classifier

Port Disabled

Switch Health and Uptime

View Details

Diagnostics and Tools

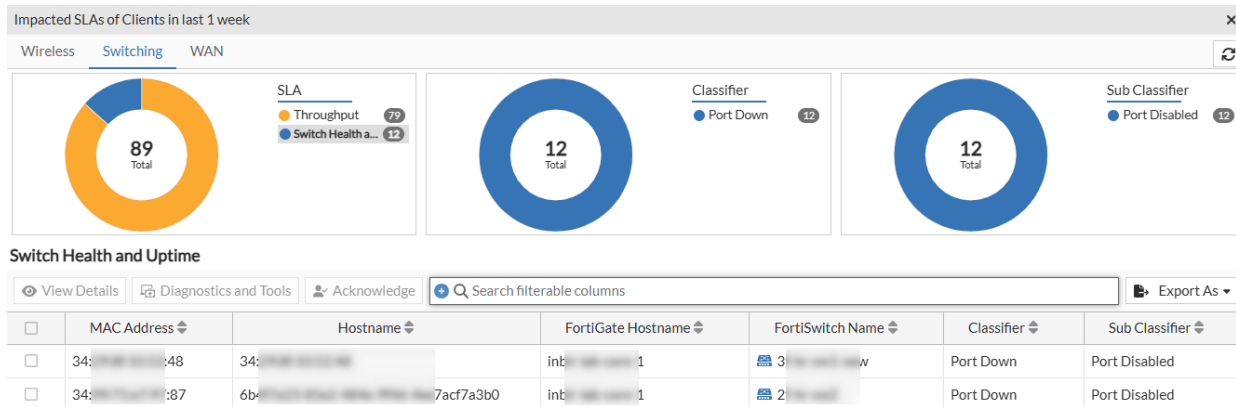
Acknowledge

Search filterable columns

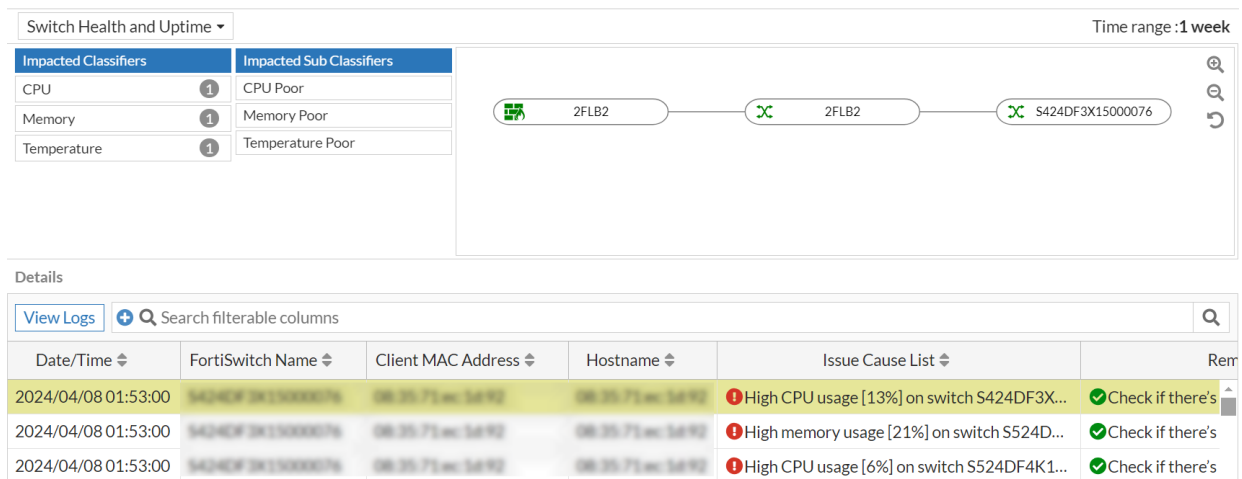
Export As

☐	FortiGate Hostname	FortiSwitch Name	OS Version	Classifier	Sub Classifier
☐	In [REDACTED]-1	[REDACTED]	S448DN [REDACTED] 3 (GA)	Port Down	Port Disabled
☐	In [REDACTED]-1	[REDACTED]	S448EN [REDACTED] 5 (GA)	Port Down	Port Disabled

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



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



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

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

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

Switch Logs		
Diagnostics		Logs
Issue Diagnostics		
Issue Cause	High CPU usage [40%] on switch switch ID: 1234567890	
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		
Diagnostics		
Logs		
Search		
Date/Time	Level	Message
2022/07/06 12:48:52	Notice	cpu value is 40

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

Switch Connection Failure

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

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

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

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

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

Switch Logs	
Diagnostics	Logs
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.

Switch Logs		
Diagnostics	Logs	
Search		
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

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

SD-WAN

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



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

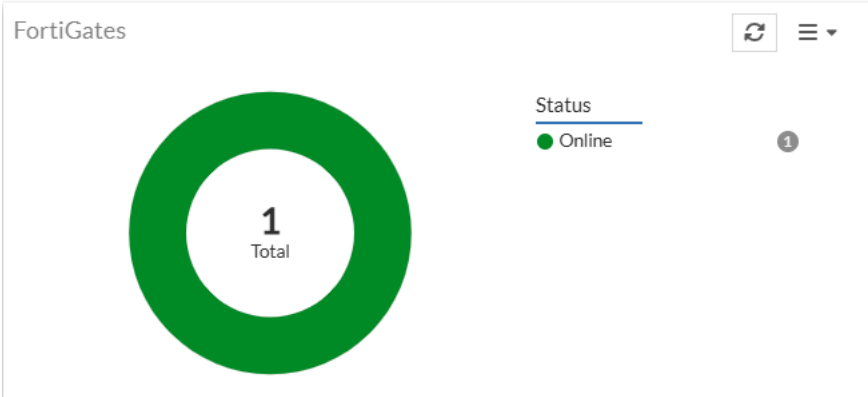
The following charts are available on the **SD-WAN** page:

- [FortiGates](#)
- [SD-WAN Health Overview](#)

- [SD-WAN Events](#)
- [SD-WAN](#)
- [Top SLA Issues](#)
- [Top Talkers](#)
- [Top Applications](#)
- [FortiExtenders](#)
- [FortiExtenders CPU Usage](#)
- [FortiExtenders Memory usage](#)

FortiGates

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



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

1

Total

Status

● Online

1

1

Total

FortiGate Model

● FortiGate-300E

1

1

Total

OS Version

● v7.6.1

1

View details

Search filterable columns

Q

+ Add

Edit

Delete

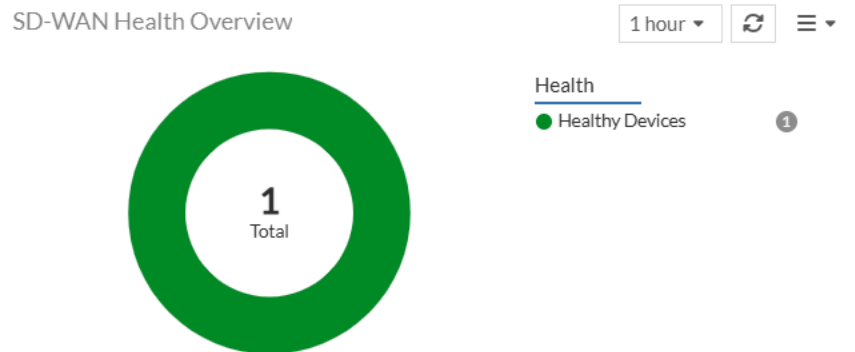
Actions

Export As

	FortiGate Name	FortiGate IP Address	Status	Discovery State	Uptime	Cluster Name	HA Mode	License	DNS Hostname
☐	office	10.0.0.1	● Online	Successfully Discovered	0d:18h:47m:47s		Standalone	Monitoring Analytics SD-WAN ● Licensed ● Licensed ● Licensed	

For more information, see [Managing FortiGates](#).

SD-WAN Health Overview



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

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

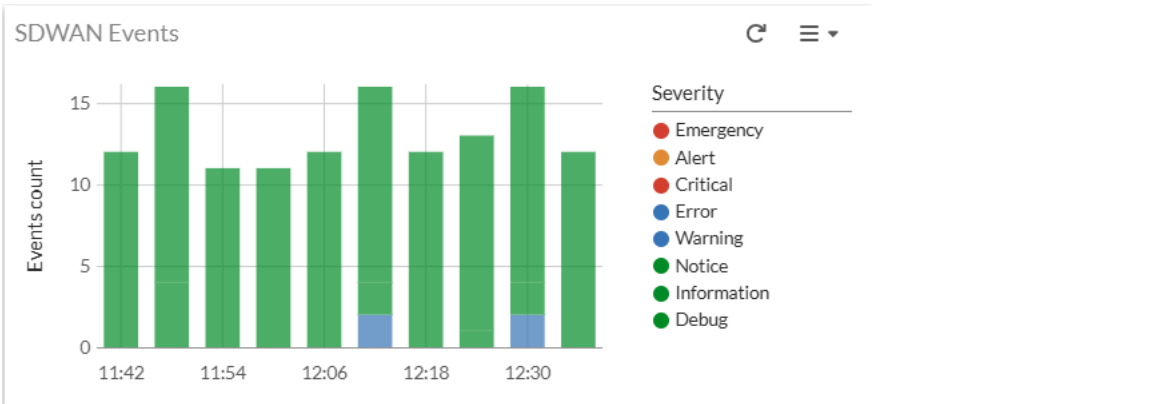
Clicking on each value displays a detailed table with information such as the hostname, up time, average latency, average jitter, and average packet loss.

Health Overview ×					
Search filterable columns Q					
☐	Hostname 	Up Time 	Average Latency 	Average Jitter 	Average Packet Loss 
☐	 offi...	● 97.7%	8.48ms	0.16ms	0.08%

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

SD-WAN Events

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



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

SDWAN Events									
Level == Warning Hostname == Pune-Core1 Interface == port2,port1,twn_advpn1_4 Search filterable columns Details									
	Date/Time	Level	Log Description	Message	Log ID	FortiGate Serial Number	Hostname	Interface	Health Check
☒	2025/03/28 12:32:16	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.
☐	2025/03/28 12:32:14	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.
☐	2025/03/28 12:12:44	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.
☐	2025/03/28 12:12:41	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.

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

SDWAN Events

Level == Warning Hostname == Pune-Core1 Interface == port2,port1,twn_advpn1_4 Search filterable columns Details

	Date/Time	Level	Log Description	Message	Log ID	FortiGate Serial Number	Hostname	Interface	Health Check
☒	2025/03/28 12:32:16	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.
☐	2025/03/28 12:32:14	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.
☐	2025/03/28 12:12:44	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.
☐	2025/03/28 12:12:41	Warning	SDWAN SLA information warning	SD-WAN health-check member changed state.	0113	4	Pune-Core1	port2	SD-WAN health-check member changed state.

General

Absolute Date/Time2025/03/28 12:32:16

Time12:32:17

Virtual Domainroot

Log DescriptionSDWAN SLA information warning

Source

Interfaceport2

Health CheckSD-WAN health-check member changed state.

Message

MessageSD-WAN health-check member changed state.

Security

LevelWarning

Other

Log event original timestamp17

Timezone+0530

Log ID0113

Typeevent

Sub Typesdwan

JitterN/A

LatencyN/A

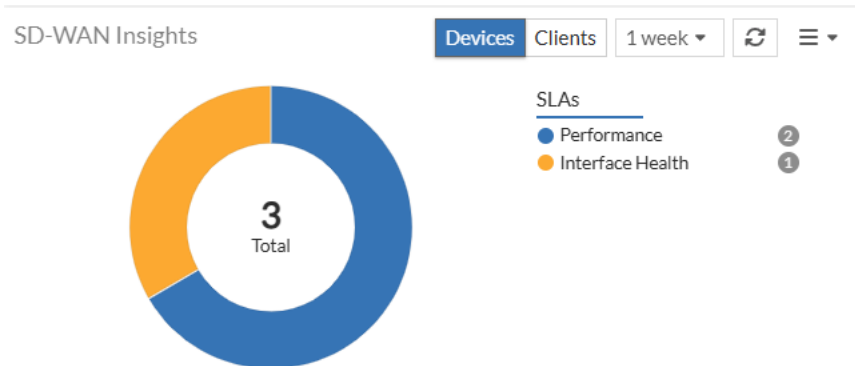
Packet LossN/A

4 Updated: 13:00:27

Close

SD-WAN Insights

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



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

Topology and Logs

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

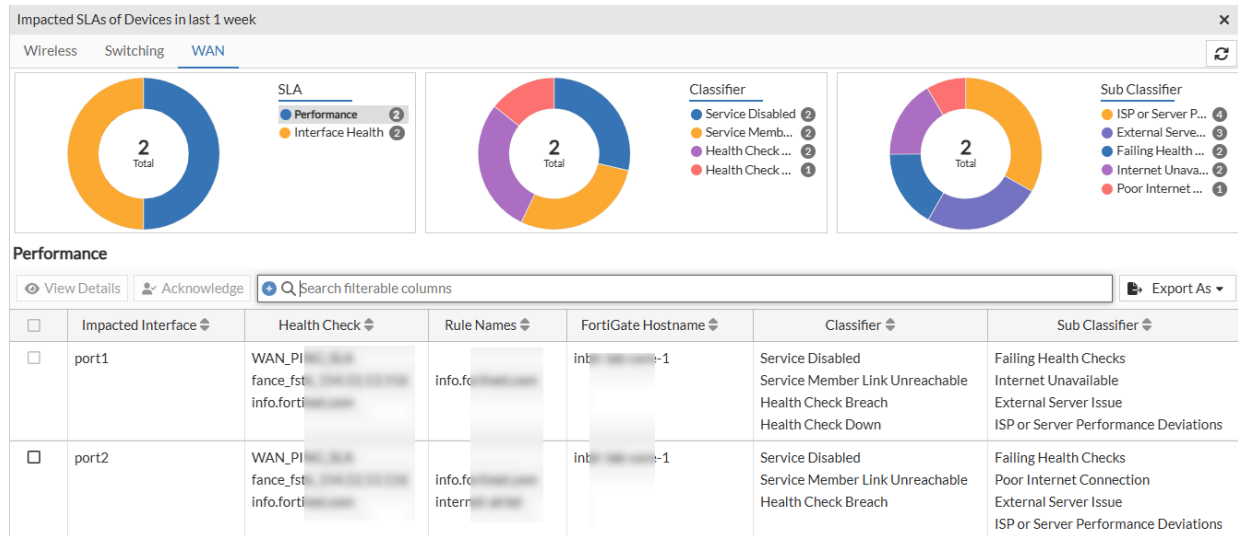
Performance SLA

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

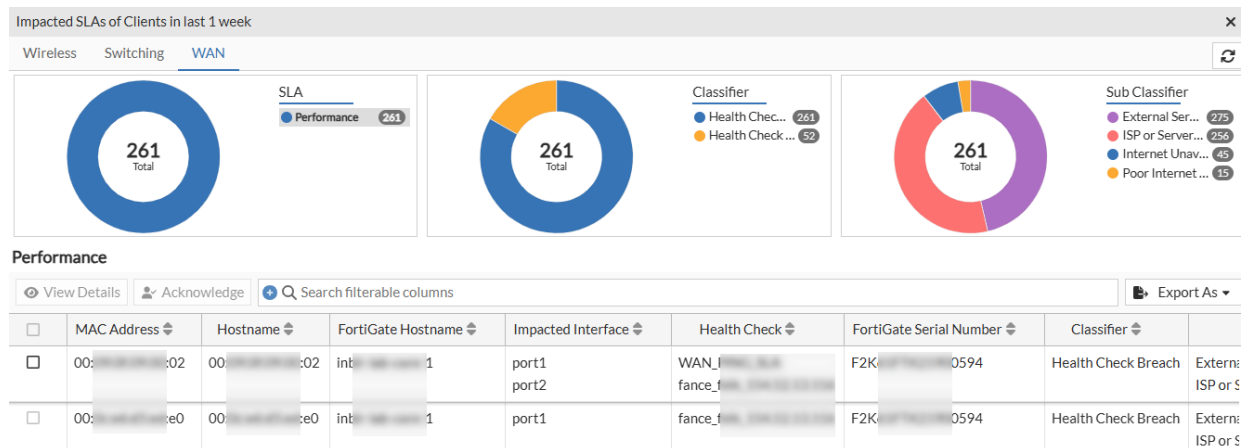


It is recommended to retain the default configurations for Link Status configuration in FortiGate monitored Performance SLAs. Aggressively configured values may lead to the generation of excessive failure alerts.

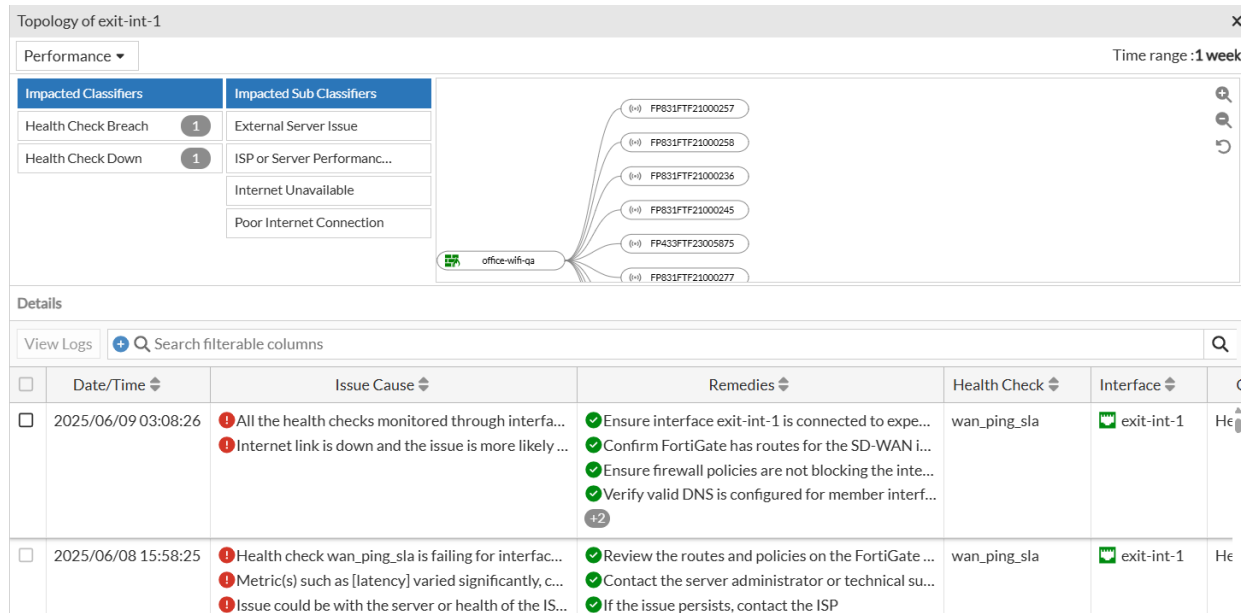
If you select the **Devices** view in the SD-WAN panel and click on the Performance SLA in the impacted SLAs list or click on the bar in the chart, the impacted interfaces' details such as, destination interface, the associated FortiGate host name, IP address, and serial number, FortiSwitch serial number,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



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



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



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

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

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

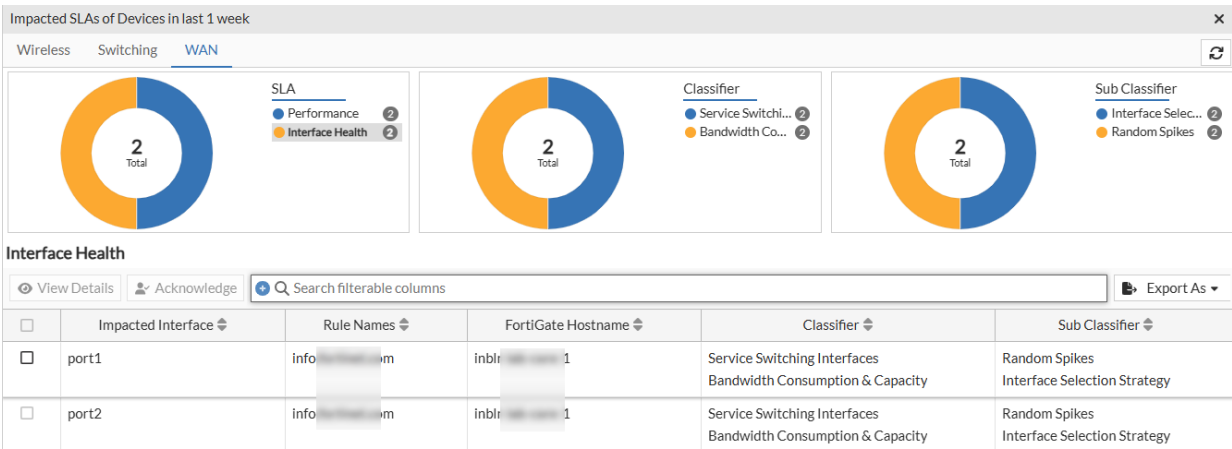
Select a row from the table and click **View Logs** to view further details.

Device Details		×
Diagnostics SD-WAN Logs System Logs VPN Logs		
Issue Diagnostics		
Issue Cause	- Health check wan_ping_sla is failing for interface exit-int-1 with 100% packet loss - Note that the health check had passed sometime in the past for the same server "8.8.8.8" - The server unreachability issues could be specific to the server, application or protocol being used in the health check, or due to any of the issues such as - network congestion on the path, link latency, firewall or security feature blocking the connection or server side problems, etc.	
Remedy	- Validate reachability of the server from the affected SD-WAN interface using the desired protocol - Contact the server administrator or technical support to check if the server is overloaded, under maintenance, or upgrades and evaluate if alternate servers can be used in the meantime - If the issue persists or if the server is reachable from any other interfaces, contact the ISP	

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

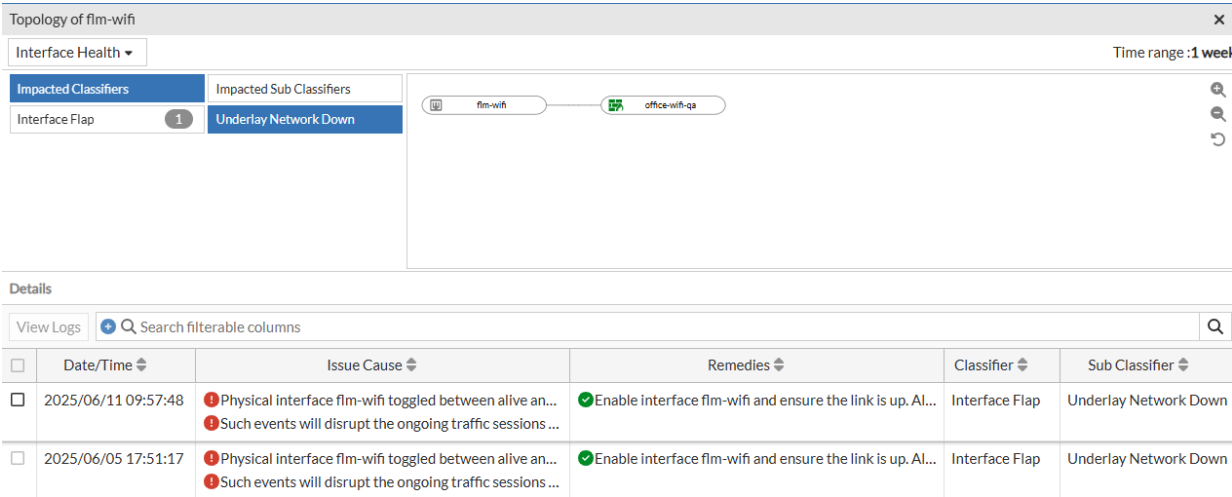
Interface Health SLA

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



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

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



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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Issue Cause	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
End Timestamp	End time of the impact based on your timezone.
In Bandwidth	Bandwidth of the incoming data.

Attribute	Description
Interface	The interface name for the reported issue.
Out Bandwidth	Bandwidth of the outgoing data.
Rule Name	The name of the rule to track the interface failure.
Tunnel Interface	Name of the tunnel interface.

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

Device Details
×

Diagnostics
SD-WAN Logs
System Logs
VPN Logs

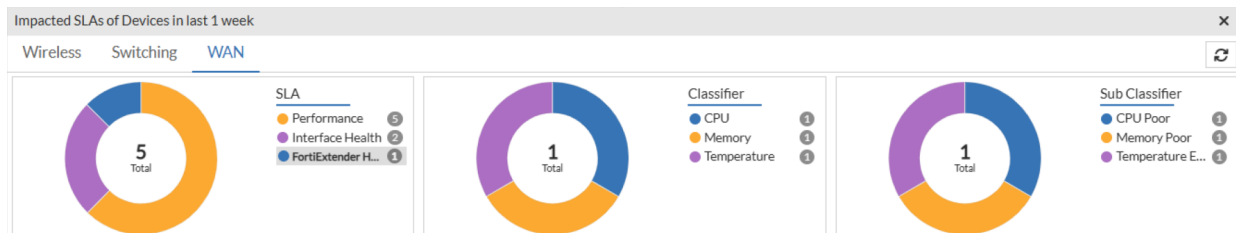
Issue Diagnostics

Issue Cause	- Physical interface flm-wifi toggled between alive and dead status atleast 1 times within 60 seconds, primarily due to interface config changes - Such events will disrupt the ongoing traffic sessions and degrade the system performance and user experience
Remedy	Enable interface flm-wifi and ensure the link is up. Also, avoid such frequent changes to interface's config

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

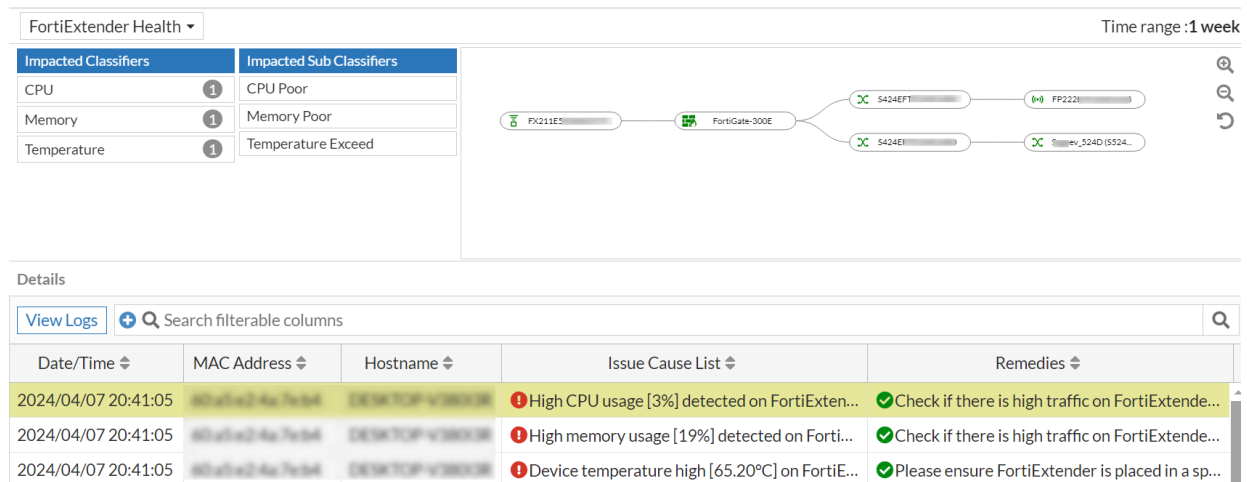
FortiExtender Health SLA

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



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

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



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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiGate Serial Number	The serial number of the associated FortiGate.
AP Serial	The serial number of the associated AP.
Access Point	The name of the associated AP.
MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
Issue Cause List	The detailed cause of the SLA breach that impacted the client/AP/FortiGate/FortiExtender.
Remedies	The suggested remedies to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Source and Destination Interface	The SD-WAN interface name.
FortiSwitch Serial Number	The serial number of the impacted switch.
FortiSwitch Name	The name of the impacted switch.
FortiExtender Serial Number	The serial number of the impacted FortiExtender.
FortiExtender Name	The name of the impacted FortiExtender.
FortiGate Hostname	The hostname of the FortiGate with which the impacted FortiExtender is associated.
Client Type	The client type that is impacted, wireless or wired.

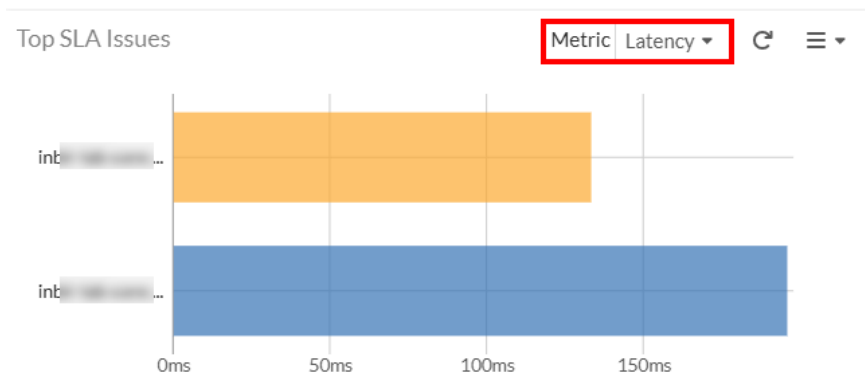
Select a particular client and click **View Logs**, to view the impacted client logs.

Client Details ×							
CLIENT LOGS							
Search							
Date/Time	Health Check	Interface	Status	Latency	Jitter	Packet Loss(%)	
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

Top SLA Issues

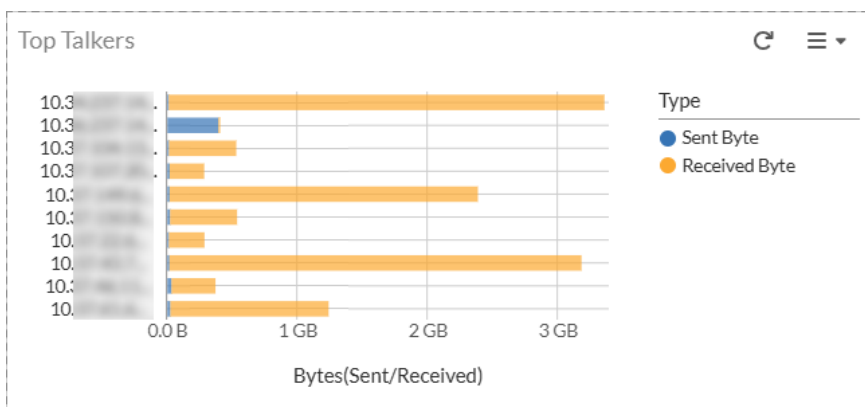
This chart displays the top 10 worst SD-WAN performance values for each metrics for Interfaces—Latency, Jitter, and Packet Loss for the selected time period.

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



Top Talkers

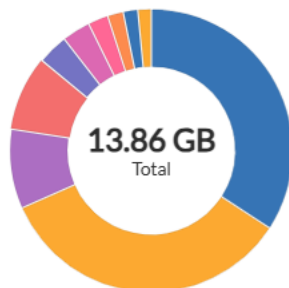
This chart displays the sources which have top 10 bandwidth usage (bytes sent and bytes received) on the SD-WAN interfaces across the FortiGate within an ADOM. Clicking on each value opens the Top Talkers detailed chart with information such as FortiGate name, interface, application, sent byte, and received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



Top Applications

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

Top Applications



Top Apps

Google.Services	4.8 GB
HTTPS.BROWSER	4.79 GB
Microsoft.Teams_Vi...	1.25 GB
SSL_TLSv1.3.PQC	1.18 GB
SSL_TLSv1.2	467.06 MB
SSH	434.87 MB
WinSCP	303.06 MB
Microsoft.Portals	231.82 MB
Microsoft.Windo...	212.28 MB

Hovering over each value displays the Application and Used Bandwidth.

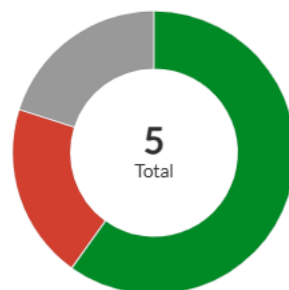
Clicking on each value opens the Top Applications detailed chart for the application displaying the FortiGate name, used bandwidth, and the interface.

Top Applications			
Search filterable columns			
☐	Hostname	Used Bandwidth	Interface
☐	int-10.10.10.1	4.78 GB	port1
☐	int-10.10.10.2	10.85 MB	port2

FortiExtenders

This chart displays the total number of FortiExtenders in your network and their status.

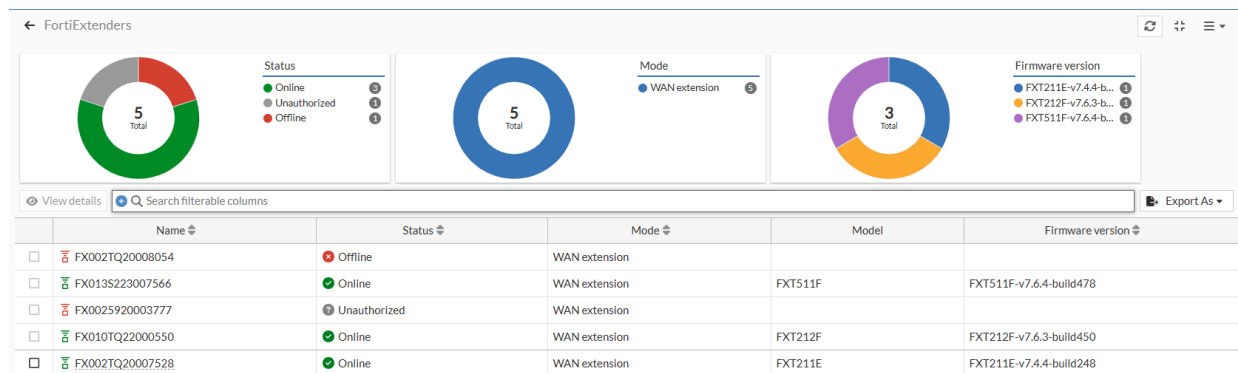
FortiExtenders



Status

Online	3
Offline	1
Unauthorized	1

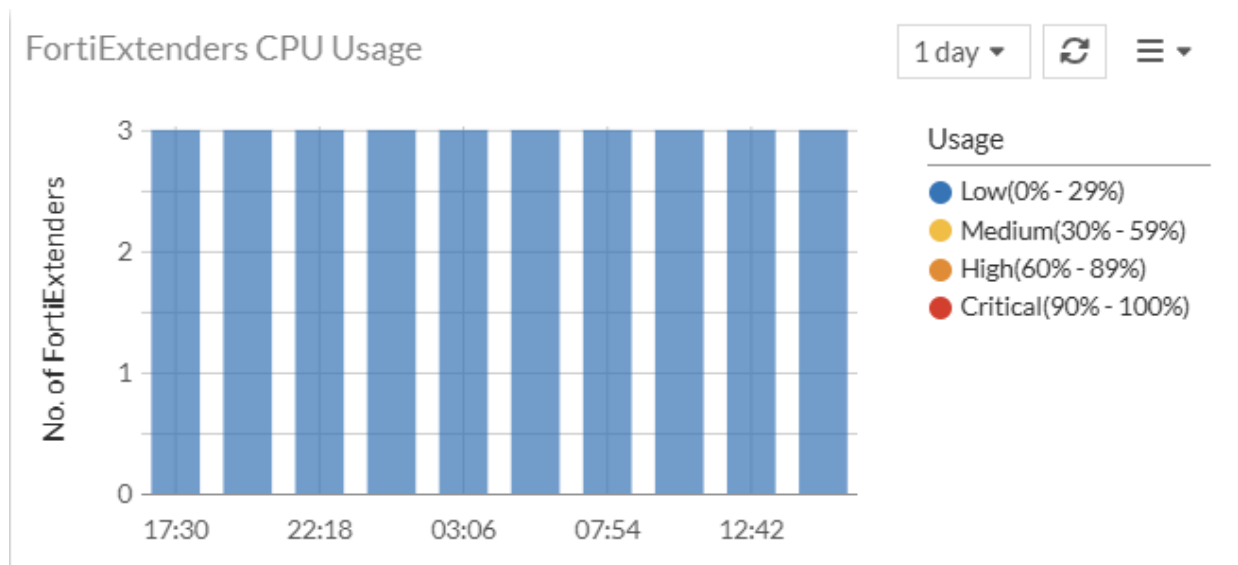
Click the chart to view more details of the FortiExtenders such as status, mode, and the firmware versions.



Select a FortiExtender device from the list and click **View Details**. The **Diagnostics and Tools** pane is displayed with more details. For more information, see [Extenders](#).

FortiExtenders CPU Usage

The FortiExtenders CPU Usage chart displays the CPU usage of the FortiExtenders over a period of time.



Click on a value on the chart to view more details on the **FortiExtender Details** pane.

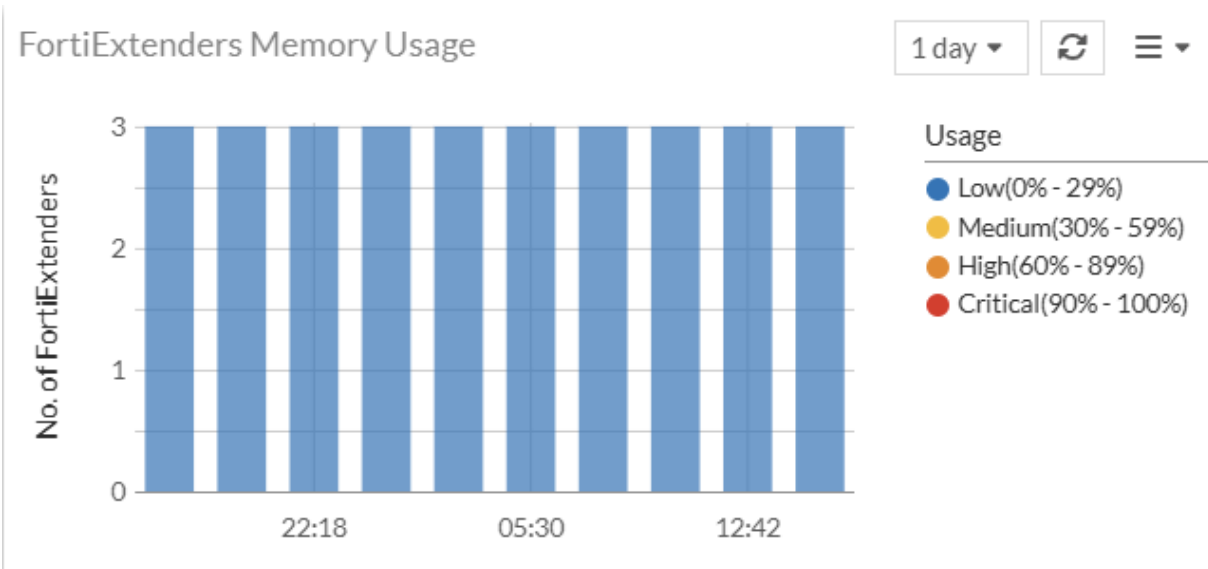
FortiExtender Details

CPU Usage = 0 -> 29 | Search filterable columns

	Date/Time	Name	Hardware Version	Gateway	MAC Address	IPv4 Netmask	Software Version	Serial Number
☐	2025/12/10 10:17:37	FX002TQ20007528	P24254-03	0.0.0.0	e0:23:ff:96:06:f1	255.255.255.0	FXT211E-v7.4.4-build248	FX211ETQ20007528
☐	2025/12/10 10:17:40	FX010TQ22000550	P27137-01	192.168.120.1	94:f3:92:27:d4:90	255.255.255.0	FXT212F-v7.6.3-build450	FX212FTQ22000550
☐	2025/12/10 10:17:49	FX013S223007566	P26657-01	192.168.130.1	74:78:a6:d8:a1:68	255.255.255.0	FXT511F-v7.6.4-build478	FX511FS223007566

FortiExtenders Memory usage

The chart displays the memory usage of the FortiExtenders in your network over a period of time.



Click on a value on the chart to view more details on the **FortiExtender Details** pane.

FortiExtender Details								
Memory Usage = 0 -> 29 ▾ 🔍 Search filterable columns								
	Date/Time ▾	Name ▾	Hardware Version ▾	Gateway ▾	MAC Address ▾	IPv4 Netmask ▾	Software Version ▾	Serial Number ▾
☐	2025/12/10 15:05:20	FX002TQ20007528	P24254-03	0.0.0.0	e0:23:ff:96:06:f1	255.255.255.0	FXT211E-v7.4.4-build248	FX211ETQ20007528
☐	2025/12/10 15:05:29	FX010TQ22000550	P27137-01	192.168.120.1	94:f3:92:27:d4:90	255.255.255.0	FXT212F-v7.6.3-build450	FX212FTQ22000550
☐	2025/12/10 15:05:33	FX013S223007566	P26657-01	192.168.130.1	74:78:a6:d8:a1:68	255.255.255.0	FXT511F-v7.6.4-build478	FX511FS223007566

Custom Dashboard

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

The following customizations are available:

- [Creating a New Dashboard](#)
- [Modifying an Existing Dashboard](#)
- [Deleting a Dashboard](#)
- [Rearranging the Dashboards](#)
- [Resetting the Dashboard Section](#)

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

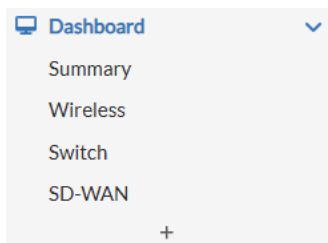
The widget library has also been improved for a more seamless user experience. For more information, see [Managing Dashboard Widgets](#).

Creating a New Dashboard

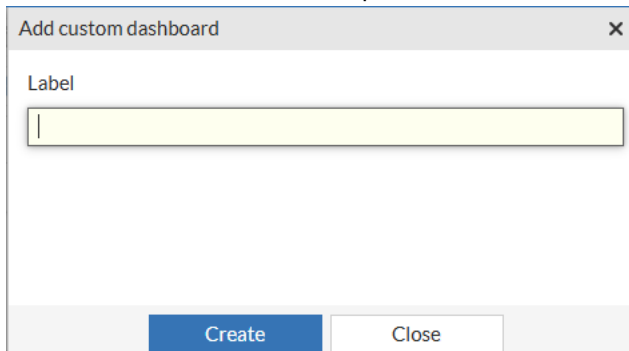
You can now create new custom dashboards and add widgets from the widget library.

To create a new dashboard:

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



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



3. Click **Create**.
Add widgets to the newly created dashboard. See [Modifying an Existing Dashboard](#).

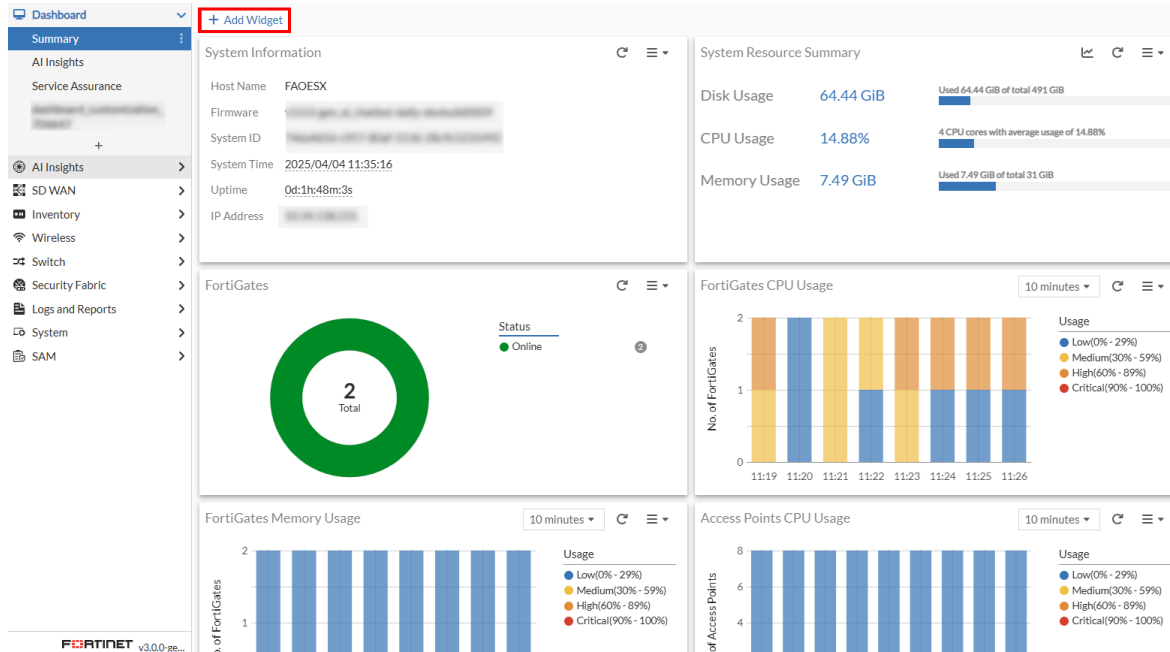
Modifying an Existing Dashboard

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

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

To add a widget to the dashboard:

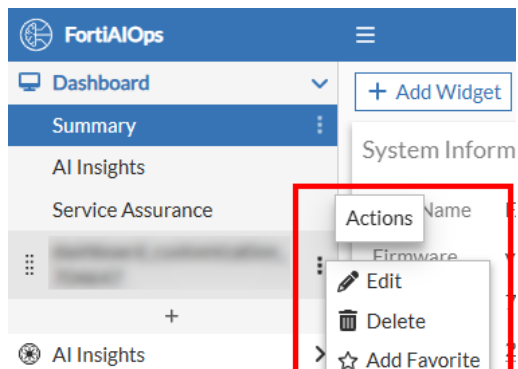
1. Select the dashboard you want to modify.
2. Click **Add Widget** to add required widgets from the widget library.



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

To change the name/label of the dashboard:

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



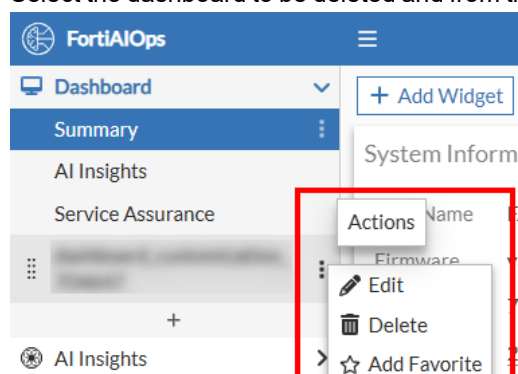
2. Change the name of the dashboard in the **Label** field and click **Update**.



Deleting a Dashboard

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

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



Note: Dashboards once deleted cannot be recovered.

Rearranging the Dashboards

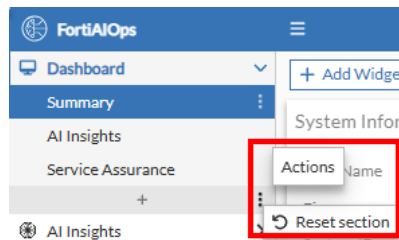
You can move a dashboard up or down to rearrange the dashboard list.

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

Resetting the Dashboard Section

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

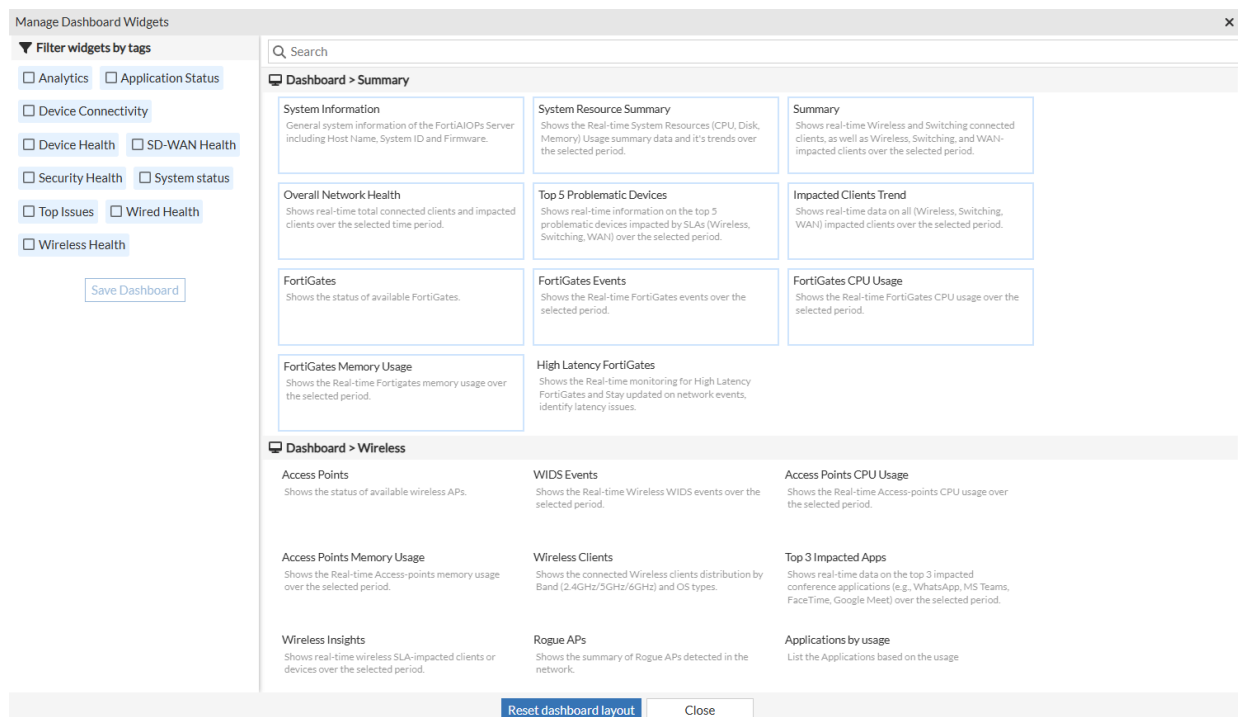
Hover over **+** and from the **Actions** menu, click **Reset section**.



Managing Dashboard Widgets

The Manage Dashboard Widgets window lists all available widgets for your dashboard in one place. Widgets are organized into categories such as Monitoring, AI-Insights, Service Assurance, SD-WAN, and Licensing.

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



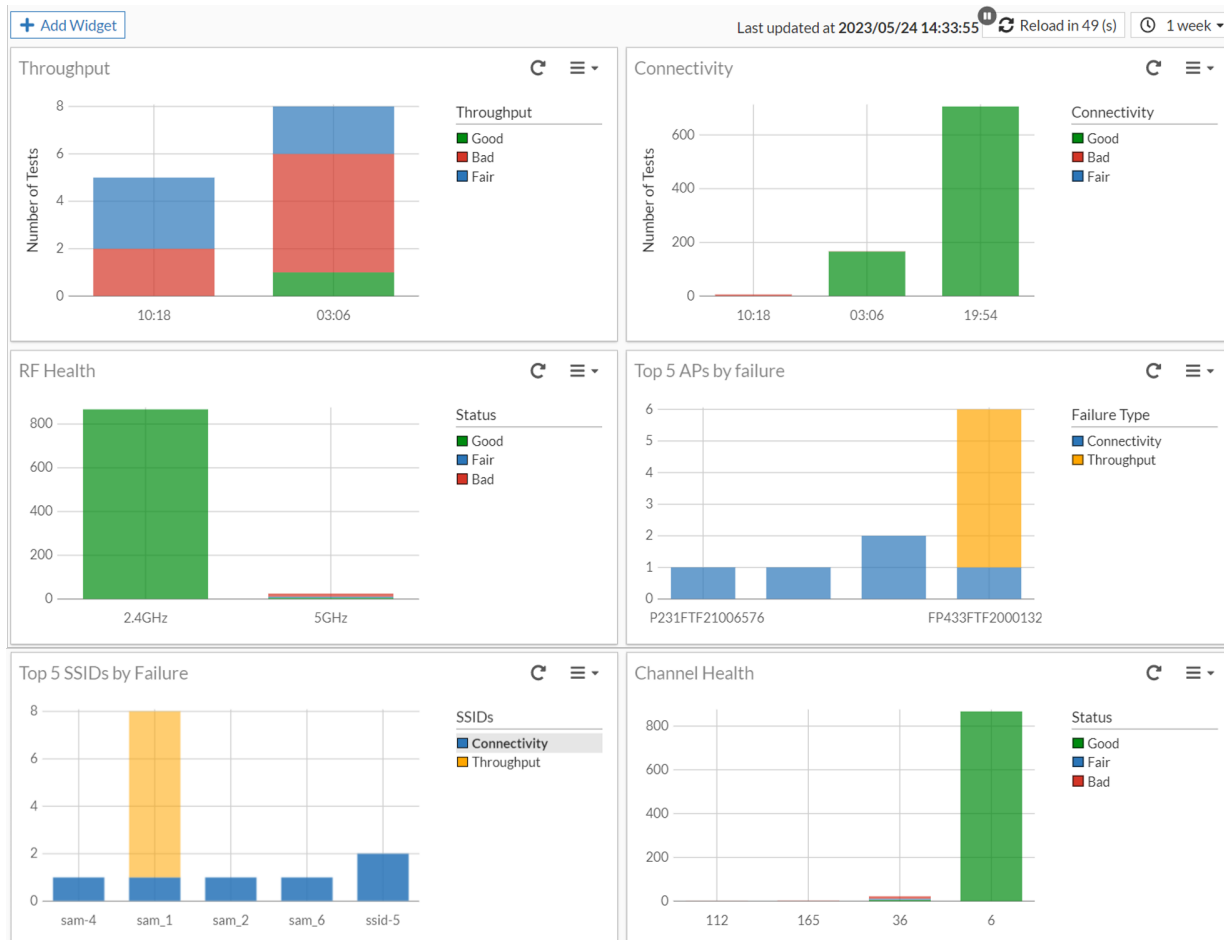
To clear all the widgets added to the dashboard, click **Reset dashboard layout**.

The widgets are categorized into the following sections:

- [Summary](#)
- [Wireless](#)
- [Switch](#)
- [SD-WAN](#)
- [Applications](#)
- [Licensing](#)
- [Service Assurance](#)

Service Assurance

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



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

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

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

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

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

+

Search

Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_thru	Throughput	FP4-10-2024-001	1	6	2	5GHz	sam-thru-base

Best Fit Columns

Reset Table

Select Columns

✓

 Test name

✓

 Test Type

✓

 AP name

✓

 SSID

✓

 Radio ID

✓

 Band

✓

 Serial Number

✓

 Baseline Name

✓

 Channel

✓

 Status

✓

 Start Time

✓

 Packet Loss

✓

 Throughput

Apply

Cancel

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, <i>throughput</i> or <i>connectivity</i> .
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, <i>2.5 GHz</i> or <i>5 GHz</i> .
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, <i>Good</i> , <i>Fair</i> , or <i>Bad</i> .
Start Time	The timestamp indicating when the test was initiated.

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

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

Connectivity							
+ Q Search							
Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP4 1051	sam 36	2	5GHz		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							
+ Q Search							
Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP4 1051	sam 36	2	5GHz		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							
+ Q Search							
Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_thru	Throughput	FP4 1051	sam 36	2	5GHz		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							
+ Q Search							
Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP4 1051	sam 36	2	5GHz		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							
+ Q Search							
Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP4 1051	sam 36	2	5GHz		sam_conn_base

AI Insights

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

- [Impacted SLA](#)
- [Impacted Devices](#)
- [SLA Config](#)

Impacted SLA

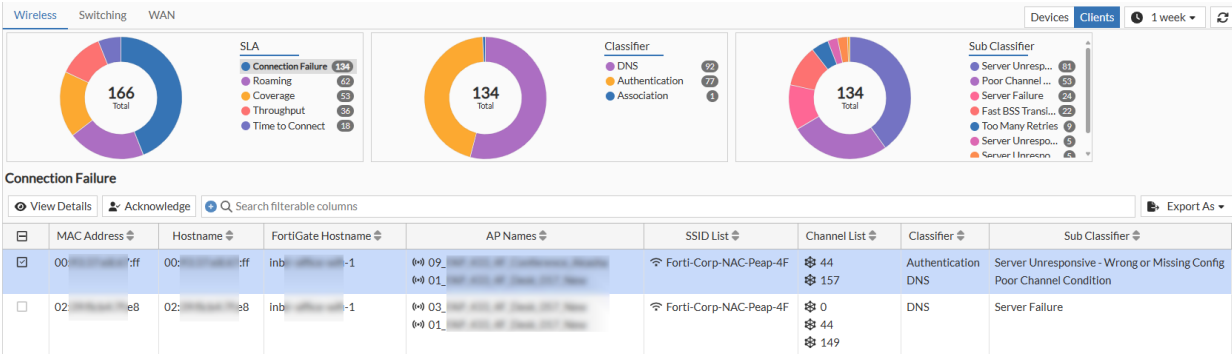
The Impacted SLA page displays the impacted wireless, switching, and WAN clients, categorized based on their SLAs, classifiers, and sub-classifiers. Select any SLA and the associated classifier and sub-classifier charts are displayed. You can filter and view the SLAs as per any of these categories. In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

Acknowledge

Network monitoring systems can generate a lot of alerts. Some of these are critical, but many can be false positives, known issues, or non-critical events. The **Acknowledge** option allows you to mark these alerts as acknowledged. By acknowledging an alert, you effectively suppress it from triggering further notifications and prevent it from negatively impacting SLA metrics for the associated devices.

For example, if FortiAI Ops reports a throughput issue because of an old 802.11b device, but you know this device is necessary for your network, you can simply acknowledge the alert. This tells the system that you have reviewed the issue and determined that it is not a real problem.

You can use the **Acknowledge** option to set up new acknowledgements.



Select the **SLA** and click **Acknowledge** to open the **Acknowledge Setting** window.

The Acknowledge Setting panel is shown on the right, with the following fields:

- Name: Acknowledge config name
- SLA Name: Connection Failure
- Sub Classifier: Server Unresponsive - Wrong or Missing Config
- Fortigate: All
- AP: All
- SSID: All
- Time Duration: Forever
- Action: Suppress

The background shows a table of Connection Failure events with columns: MAC Address, Hostname, FortiGate Hostname, AP Names, and SSID List.

Here you can set up acknowledgement rules with specific time and event scopes and choose how long an acknowledgement remains active.

- **Sub-Classifer:** Select a Sub-classifier to suppress all future alerts with a particular sub-classifier across your entire network.
- **FortiGate:** Choose between All FortiGates in your network or a specific FortiGate.
- **AP:** Select All or a specific AP.
- **SSID:** Select All or a specific SSID.
- **Time Duration:** Select Forever to retain the acknowledgement in effect until you manually revoke it or click **Select Duration** to set a custom time period for the acknowledgement to be valid.

Click **Submit** to save the changes.

Export As

The **Export As** option supports a wide range of file formats. You can export system information in CSV, JSON, Plaintext, or PDF formats for easier reporting and offline analysis.

Wireless

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

The Wireless tab displays three donut charts for SLA data:

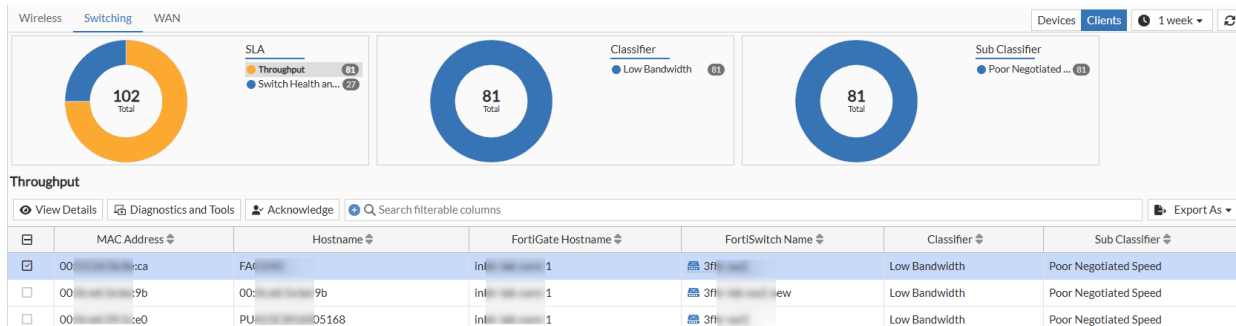
- Connection Failure: 166 Total
- DNS: 134 Total
- Authentication: 134 Total

Below the charts is a table of Connection Failure events with columns: MAC Address, Hostname, FortiGate Hostname, AP Names, SSID List, Channel List, Classifier, and Sub Classifier.

MAC Address	Hostname	FortiGate Hostname	AP Names	SSID List	Channel List	Classifier	Sub Classifier
00:00:00:00:00:00	00:00:00:00:00:00	Int-1	09, 01, 03, 01	Forti-Corp-NAC-Peap-4F	44, 157	Authentication	Server Unresponsive - Wrong or Missing Config
02:00:00:00:00:00	02:00:00:00:00:00	Int-1	03, 01	Forti-Corp-NAC-Peap-4F	0, 44, 149	DNS	Server Failure

Switching

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



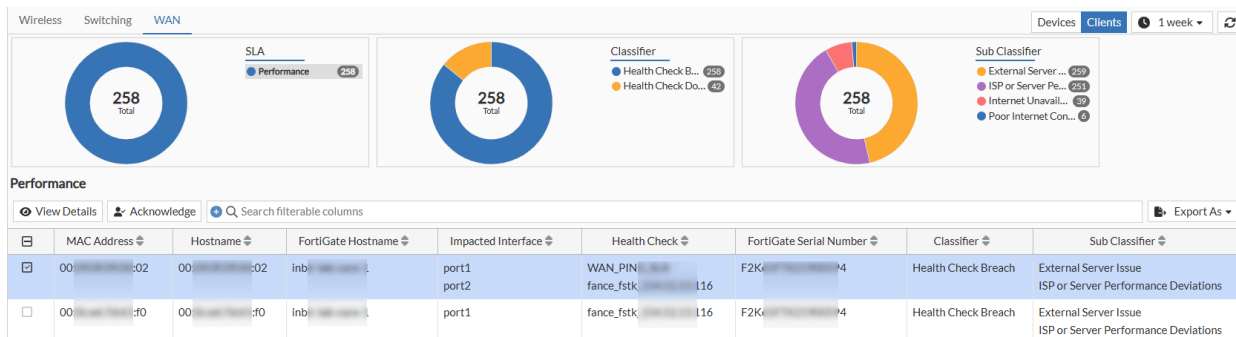
To view FortiSwitch statistics and diagnostics in detail, select a row and click **Diagnostics and Tools**. For more information, see [FortiSwitch Diagnostics and Tools](#).

WAN

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

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

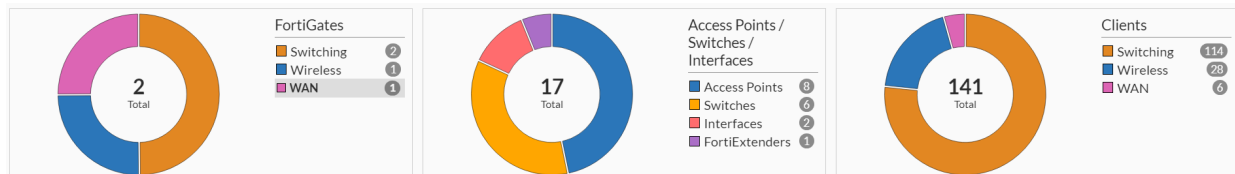
Note: To ensure the charts display accurate values, configure the necessary prerequisites and consider the recommendations provided. For more information, see [SD-WAN](#).



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

Impacted Devices

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



FortiGates

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

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

FortiGates Wireless SLA				
+ Search filterable columns				
Impacted SLAs	FortiGate Serial Number	IP Address	Impacted APs	Impacted Clients
FGVM04 6				
Connection Failure	FGVM04-300E	10.34.139.200	7	14
Time to Connect	FGVM04-300E	10.34.139.200	7	13
Throughput	FGVM04-300E	10.34.139.200	7	12

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

FortiGates WAN SLA							
+ Search filterable columns							
Impacted SLAs	FortiGate Serial Number	IP Address	Impacted APs	Impacted Switch	Impacted Interfaces	Impacted Clients	Extenders
FortiGate-300E 2							
Performance	FG300E-300E	10.34.139.200	7	1	2	6	0
FortiExtender Health	FG300E-300E	10.34.139.200	6	1	1	4	1

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

FortiGates Switching SLA

+ Search filterable columns				
Impacted SLAs	FortiGate Serial Number	IP Address	Impacted Switch	Impacted Clients
1				
Switch Health and Uptime	FGVM04TH20000176		1	5
FGT_BACKUP_182 1				
Switch Health and Uptime	FGVM04TH20000182	10.34.139.182	1	12
FGT_PRIMARY_181 1				

Access Points/ Switches/ Interfaces/FortiExtenders

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

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

+ Search filterable columns						
Impacted SLAs	Access Point	FortiGate Serial Number	FortiGate IP Address	AP Serial Number	AP IP Address	Impacted Clients
FGVM04TH20000176 24						
Connection Failure	FGVM04TH20000176	FGVM04TH20000182	10.34.139.207	FGVM04TH20000176	10.37.26.15	10
Time to Connect	FGVM04TH20000176	FGVM04TH20000182	10.34.139.207	FGVM04TH20000176	10.37.26.15	8
Time to Connect	FGVM04TH20000182	FGVM04TH20000182	10.34.139.207	FGVM04TH20000182	10.37.26.15	7

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

+ Search filterable columns				
Impacted SLAs	FortiGate IP Address	FortiGate Serial Number	Interface	Impacted Clients
FortiGate-300E 2				
Performance	10.34.139.230	FGVM04TH20000182	FEXWAN1	6
Performance	10.34.139.230	FGVM04TH20000182	port15	6

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

+ Search filterable columns							
Impacted SLAs	Name	OS Version	Connecting From	State	Status	FortiSwitch Serial Number	FortiGate Serial Number
1							
FGT_BACKUP_182 1							
Switch Health and Uptime	S248EF-v7.4.0-build767,230602 (GA)	169.254.2.2	Authorized	Connected	10.34.139.182	FGVM04TH20000182	FGVM04TH20000176
FGT_PRIMARY_181 1							
Switch Health and Uptime	S248EF-v7.4.0-build767,230602 (GA)	169.254.2.2	Authorized	Connected	10.34.139.182	FGVM04TH20000182	FGVM04TH20000176

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

FortiExtenders						
Search filterable columns						
Impacted SLAs	FortiExtender Serial	FortiExtender Name	FortiGate IP Address	FortiGate Serial Number	Interface	Impacted Clients
FortiGate-300E 1						
FortiExtender Health	FG213E1P20000777	FG213E1P20000777	10.34.139.230	FG204E161P000000	FEXWAN1	4

Clients

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

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

Wireless Clients						
Search filterable columns						
Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	AP Serial Number	Access Point	AP IP Address
FGVM04 43						
Connection Failure	Aa:21:4a:af:aa:41	FG204E161P000000	10.34.139.207	FP423E161P000076	FP423E161P000076	10.37.28.15
Connection Failure	Aa:21:4a:af:aa:41	FG204E161P000000	10.34.139.207	FP423E161P000073	FP423E161P000073	10.37.28.7
Time to Connect						
AP Health and Uptime						
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 on the impacted SLA name to view the topology.

WAN Clients						
Search filterable columns						
Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	AP Serial Number	FortiSwitch Serial Number	Access Point
FortiGate-300E 47						
Performance	aa:5f:9b:4b:13:4d	FG204E161P000000	10.34.139.230	FP233E161P000095		FP233E161P000095
Performance	7a:64:3a:f5:a5:32	FG204E161P000000	10.34.139.230	FP233E161P000076		Supernode_233
Performance	8d:c5:a2:4a:7a:64	FG204E161P000000	10.34.139.230	FP423E161P000073	8d:c5:a2:4a:7a:64	FP423E161P000073
FortiExtender Health						

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

Switching Clients						
Search filterable columns						
Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	FortiSwitch Name	FortiSwitch Serial Number	Connecting F
5						
Switch Health and Uptime	8d:c5:a2:4a:7a:64	FG204E161P000000		Supernode	8d:c5:a2:4a:7a:64	8d:c5:a2:4a:7a:64
Switch Health and Uptime	aa:23:9f:97:aa:28	FG204E161P000000		Supernode	8d:c5:a2:4a:7a:64	8d:c5:a2:4a:7a:64
Switch Health and Uptime	aa:23:9f:97:aa:28	FG204E161P000000		Supernode	8d:c5:a2:4a:7a:64	8d:c5:a2:4a:7a:64

SLA Config

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

- [Device Health](#)
- [Time To Connect](#)
- [Roaming](#)

Device Health

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

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

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

- **Temperature**

AP Health**Switch Health****FortiExtender Health**

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

Time To Connect

You can configure static thresholds or enable FortiAI Ops 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.

Time to Connect
Roaming

☒ Dynamic Baselines Configuration

Scope
Device Group
FortiGate
AP

Time Selection
Duration
Date Range

15 Day(s)

Schedule Baselines Computation
☒
27-09-2024
0

Repeat Cycle
☒
7
Day(s)

Apply Changes

DYNAMICALLY OBTAINED BASELINES VALUES

Refresh
Recompute Baselines
+ Q Search

☐	Last Updated	FortiGate Hostname	Association	Authentication Time	DHCP Time	DNS Time
--------------------------	--------------	--------------------	-------------	---------------------	-----------	----------

- **Scope** - Select the scope to calculate the thresholds which could either be per **ADOM**, per **FortiGate**, or per **AP**.
- **Time Selection** - Set the time range/duration for which FortiAI Ops analysis client data to derive the thresholds.
- **Schedule Baselines Computation** - Set the time when FortiAI Ops 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 FortiAI Ops 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.

Time to Connect
Roaming

☒ Dynamic Baselines Configuration

Association Time
176276
ms

Authentication Time
51863
ms

DHCP Time
2000
ms

DNS Time
300
ms

Apply Changes

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

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

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

Notes:

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

Roaming

You can configure static thresholds or enable FortiAI Ops 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.

Time to Connect

Roaming

Dynamic Baselines Configuration

Scope

Device GroupFortiGateAPSSID

Time Selection

DurationDate Range

15 Day(s)

Schedule Baselines Computation

27-09-20240

Repeat Cycle

7Day(s)

Apply Changes

DYNAMICALLY OBTAINED BASELINES VALUES

Refresh

Recompute Baselines

Search

Last UpdatedAP NameFortiGate Hostname11r TimeOKC TimePMK TimeStatus

- **Scope** - Select the scope to calculate the thresholds which could either be per **ADOM**, per **FortiGate**, per **AP**, or per **SSID**.
- **Time Selection** - Set the time range/duration for which FortiAI Ops analysis client data to derive the thresholds.
- **Schedule Baselines Computation** - Set the time when FortiAI Ops 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 FortiAI Ops 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.

Time to Connect
Roaming

☒ Dynamic Baselines Configuration

Fast BSS Transition Roams(11r)	79732	ms		Low
Opportunistic Key Caching Roams(okc)	100	ms		Low
PMK Cache Roams	100	ms		Low

Apply Changes

- **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 FortiAI Ops, 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.

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

Event Acknowledgement

The **Event Acknowledgement** window lists all the acknowledgements that are configured in the system.

Favorite	✎ Edit ✖ Delete 🔍 Search
Dashboard	
AI Insights	
Impacted SLAs	
Impacted Devices	
Configurations	
SLA	
Event Acknowledgement	
Inventory	
Wireless	
Switch	
FortiExtenders	
SD-WAN	
Security Fabric	
Logs and Reports	
System	
SAM	

Name	SLA Name	Status	Access Point	Sub Classifier	Ack at	End Time
Throughput-Coverage-Hole	Throughput	Expired	5_433G-3F [redacted] 5GHz_Desk93	Coverage Hole	2025/08/28 16:35:54	2025/08/29 04:35:54
Roaming-Delay	Roaming	Expired	6.83x-3F [redacted] Desk76	Roaming Delay	2025/08/28 16:34:44	2025/08/29 04:34:44
TTC-Poorbandwidth	Time to Connect	Expired	1_83x-3F [redacted] Desk76	Poor Bandwidth	2025/08/28 16:33:01	2025/08/29 04:33:01
WAN-PERF-ISP	Performance	Expired	[redacted]	ISP or Server Performance Deviations	2025/08/26 12:24:44	2025/08/27 00:24:44
WIDS-Longduration	WIDS	Expired	Fortinet	Long Duration ID	2025/08/26 12:24:05	2025/08/27 00:24:05
Throughput-asymmetric	Throughput	Expired	1_83x-3F [redacted] Desk76	Asymmetric Data Rates	2025/08/26 12:23:41	2025/08/27 00:23:41
TTC-loadissue	Time to Connect	Expired	7_83x-3F [redacted] Desk114	Coverage or Load Issue	2025/08/26 12:23:16	2025/08/27 00:23:16
coverage-distantclient	Coverage	Expired	6.83x-3F [redacted] Desk76	Distant Client	2025/08/26 12:22:51	2025/08/27 00:22:51
connfailure-serverunres	Connection Failure	Expired	6.83x-3F [redacted] Desk76	Server Unresponsive - Wrong or Missing Config	2025/08/26 12:22:09	2025/08/27 00:22:09
Suppress-DNS-No-Domain-Events	Connection Failure	Enabled	all	No Domain		

To edit an acknowledgement, select an acknowledgement and click **Edit**. Make the following changes as required:

- **Enable/Disable** - Use this setting to temporarily pause or resume an acknowledgement.
- **Time Duration**: Select **Forever** to retain the acknowledgement in effect until you manually revoke it or click **Select Duration** to set a custom time period for the acknowledgement to be valid.

Favorite	✎ Edit ✖ Delete 🔍 Search
Dashboard	
AI Insights	
Impacted SLAs	
Impacted Devices	
Configurations	
SLA	
Event Acknowledgement	
Inventory	
Wireless	
Switch	
FortiExtenders	
SD-WAN	
Security Fabric	
Logs and Reports	
System	
SAM	

Name	SLA Name	Status	Sub Classifier	Ack at
Throughput-Coverage-Hole	Throughput	Expired	Coverage Hole	2025/08/28 16:35:54
Roaming-Delay	Roaming	Expired	Roaming Delay	2025/08/28 16:34:44
TTC-Poorbandwidth	Time to Connect	Expired	Poor Bandwidth	2025/08/28 16:33:01
WAN-PERF-ISP	Performance	Expired	ISP or Server Performance Deviations	2025/08/26 12:24:44
WIDS-Longduration	WIDS	Expired	Long Duration ID	2025/08/26 12:24:05
Throughput-asymmetric	Throughput	Expired	Asymmetric Data Rates	2025/08/26 12:23:41
TTC-loadissue	Time to Connect	Expired	Coverage or Load Issue	2025/08/26 12:23:16
coverage-distantclient	Coverage	Expired	Distant Client	2025/08/26 12:22:51
connfailure-serverunres	Connection Failure	Expired	Server Unresponsive - Wrong or Missing Config	2025/08/26 12:22:09
Suppress-DNS-No-Domain-Events	Connection Failure	Enabled	No Domain	

Edit Acknowledged Configuration

Name
Throughput-Coverage-Hole

SLA Name
Throughput

Sub Classifier
Coverage Hole

Fortigate
All office-wifi-ga

AP
5_433G-3F 5GHz_Desk93

Time Duration
Forever Select Duration

12 hours

Action
Suppress

Status
Enabled Disabled

To delete an acknowledgement, from the **Event Acknowledgement** window, select an acknowledgement and click **Delete**.

FortiAI

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

Following are some of the key capabilities of FortiAI:

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

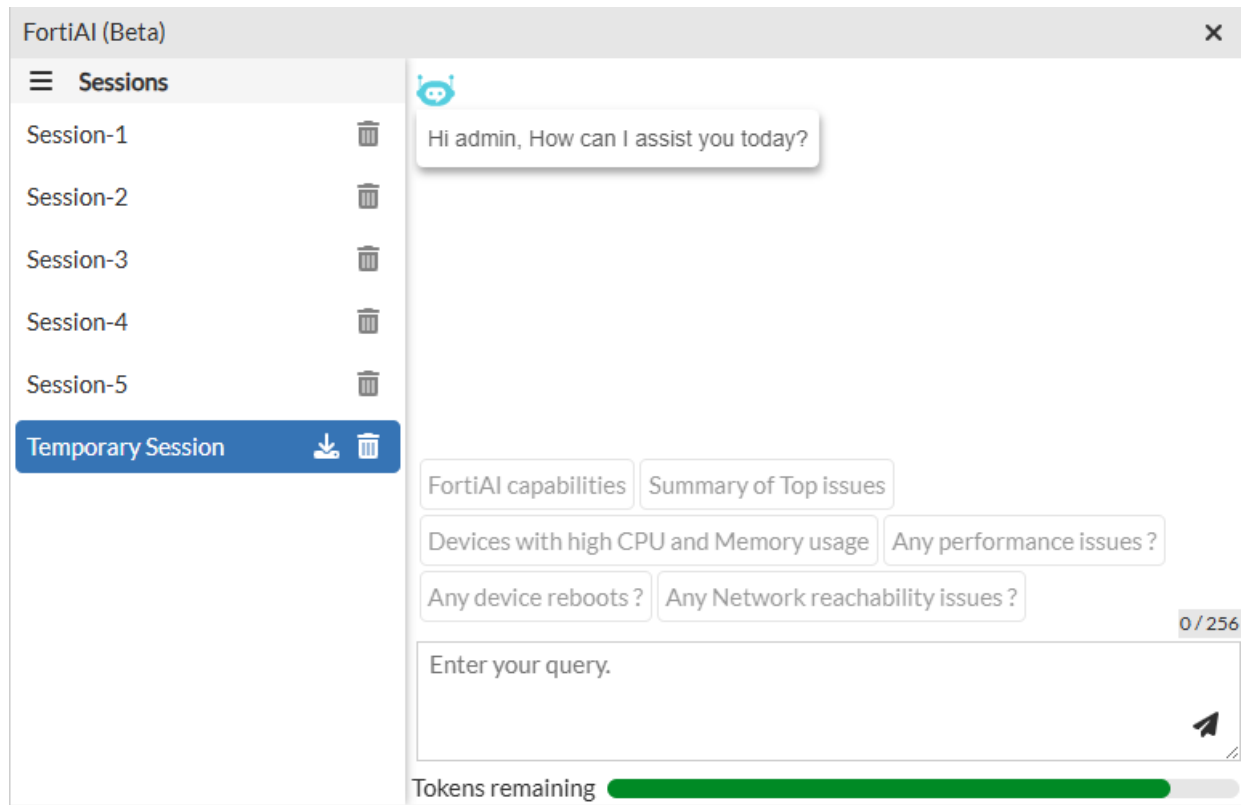


In this release, FortiAI is available to all customers as a **Beta** feature and includes a grant of 10 million tokens for use.

Accessing FortiAI

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

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



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

Using FortiAI

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

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

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

FortiAI Capabilities

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

Category	Description
Wireless Troubleshooting	Monitor access point health (power, CPU, performance), troubleshoot specific client connectivity issues, and analyze the RF environment for interference.

Category	Description
Wired Network Diagnostics	Diagnose physical layer issues such as port flaps, down ports, and cable faults, while also monitoring overall switch bandwidth and throughput performance.
SD-WAN Health	Track real-time SD-WAN health by identifying top issues, overlay failures, interface performance degradation, and recent SLA health check breaches.
Configuration and Task Support	Receive instructions for common administrative tasks, and platform configuration.
Packet Capture and Analysis	Upload PCAP files for troubleshooting network issues, initiate packet captures that can be downloaded for further analysis. Note: PCAP analysis provides an estimated accuracy of 65%. We recommend using the results as initial guidance rather than a definitive diagnosis.

FortiAI Prompts

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

Example of valid prompts:

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



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

FortiAI Pane

The FortiAI pane includes the following:

Section	Description
Sessions	Continuous conversation that maintains context, allowing you to ask follow-up questions about previously discussed information until the session ends by logging out, closing the window, or reloading.
Thread	A chronological record of prompts and responses within a single session of the FortiAI assistant.
Prompt	An instruction or question you provide to the FortiAI assistant. It can be a query that you type yourself, or a pre-defined suggestion that you select to request common information or actions.
Token remaining	Displays your current token usage out of your total allotment. For more

Section	Description
	information, see FortiAI Tokens .
Attach File	Enables you to upload PCAP file to FortiAI for further analysis.

FortiAI Data Privacy

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

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

How private data is protected

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

FortiAI Tokens

As a FortiAI Ops customer, you now have access to FortiAI as a **Beta** feature in this release. This includes an allocation of 10 million tokens for evaluation.

How token usage is calculated

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

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

Best practices

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

- Make your prompts concise and specific. Vague questions require more processing and can yield broad, less useful answers, consuming more tokens.
- Use filters in your prompts to receive concise and specific responses. Add details like time-frames, device names, or specific metrics to narrow the focus. For example, instead of "How is my network doing?", try asking "Show me the top 5 non-performing access points in the last hour."
- Use terms that directly relate to functions and metrics you see in the FortiAI Ops dashboards. This helps the assistant translate your request into a precise query much more efficiently. For example, instead of "Are any connections bad?", try "Are there any throughput SLA issues in the network?"
- Reference details in the existing thread when possible. FortiAI remembers the context of your current conversation thread. Referencing previous responses is more efficient than starting a new query.

For example, imagine the following exchange:

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

FortiAI responds with the information.

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

Viewing token usage

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

- Total Tokens
- Consumed Tokens

FortiAI Example Tasks

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

Example 1: Finding under performing Access Points

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

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

Prompt: Which APs are under performing?

12:37:18 PM

Which APs are under performing?

12:37:18 PM

Summary of Underperforming APs (Last 2 Hours):

Grouped by AP and Issue Type:

1. 1.83x-3F-4F-0A-00-00-00
 - Issues: Wi-Fi Interference, Poor Coverage, Distant Client
 - Impacted Clients: 4e:fc:b1:12:34:56, 72:22:6e:12:34:56, IND-KU-1234-5678-9012, da:c6:12:34:56:78, iPhone, etc.
 - SSIDs: Forti-Corp-Floor-1
 - Impacted Channels: 44
2. 2.FAP_433F_KK_Cube
 - Issue: Poor Coverage
 - Impacted Clients: 4e:fc:b1:12:34:56, 72:22:6e:12:34:56, IND-KU-1234-5678-9012, da:c6:12:34:56:78, iPhone, etc.
 - SSIDs: Forti-Corp-Floor-1
 - Impacted Channels: 44, 60
3. 3.83x-3F-4F-0A-00-00-00
 - Issue: Wi-Fi Interference
 - Impacted Clients: None
4. 4.83x-3F-4F-0A-00-00-00
 - Issue: Wi-Fi Interference
 - Impacted Clients: None
5. 6.83x-3F-4F-0A-00-00-00
 - Issue: Wi-Fi Interference
 - Impacted Clients: None

Key Points:

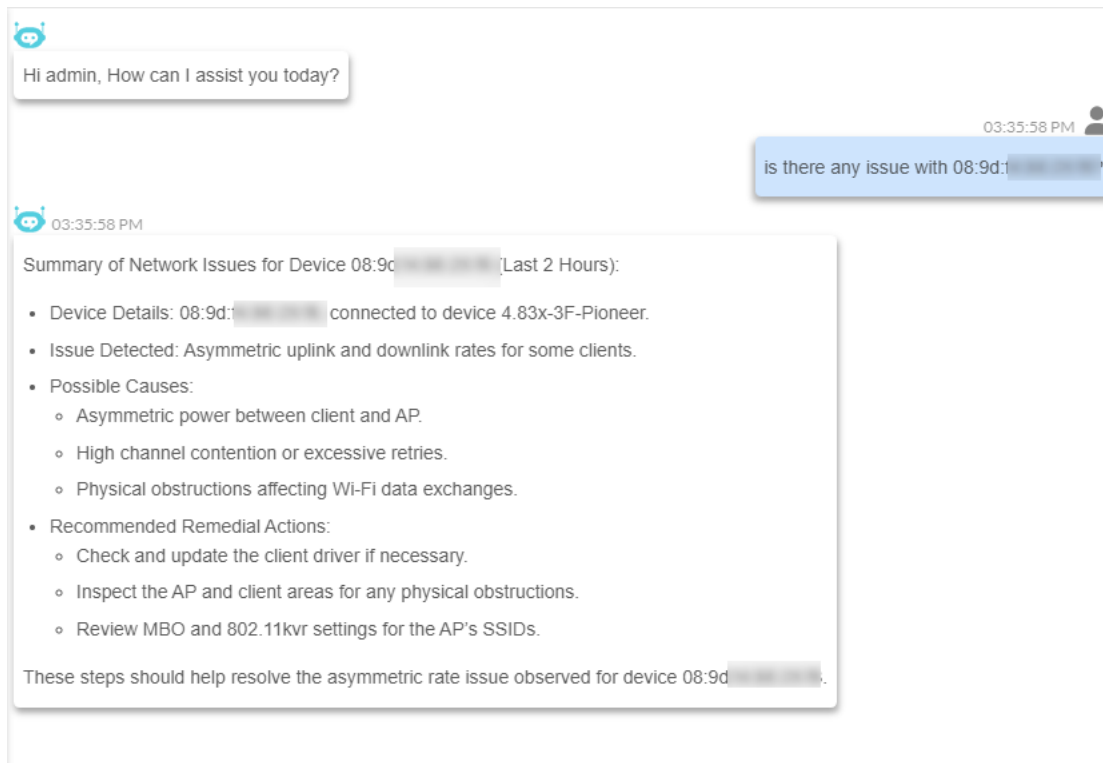
- 1.83x-3F-4F-0A-00-00-00 is experiencing multiple issues (Wi-Fi Interference, Poor Coverage, Distant Client) and is impacting several clients.
- 2.FAP_433F_KK_Cube is experiencing Poor Coverage affecting multiple clients.
- 3.83x-3F-4F-0A-00-00-00, 4.83x-3F-4F-0A-00-00-00, and 6.83x-3F-4F-0A-00-00-00 have reported Wi-Fi Interference but no impacted clients.

Etc.

Example 2: Diagnosing Device-Specific Issues

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

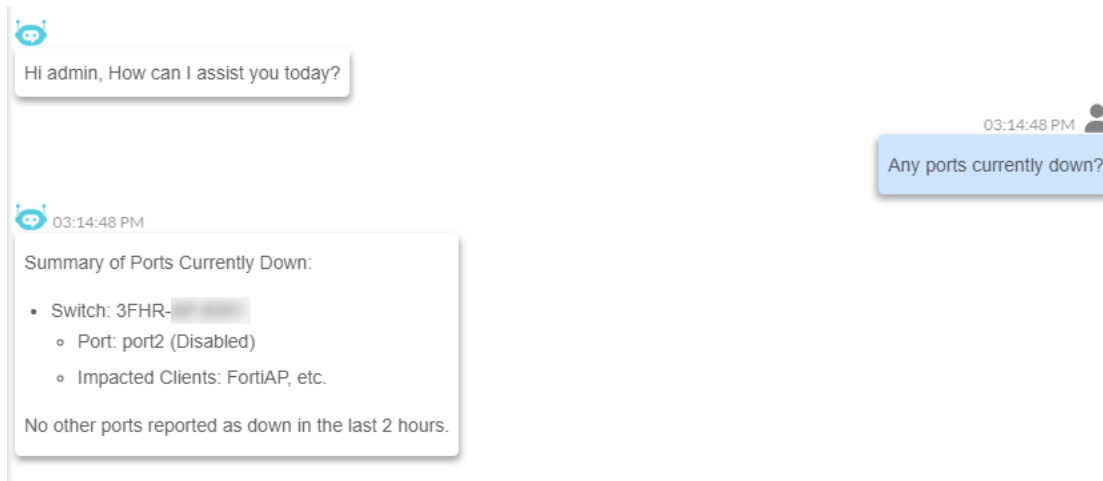
Prompt: Is there any issue with <MAC address>?



Example 3: Outage Detection and Impact Analysis

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

Prompt: Are any ports currently down?



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

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

by the SD-WAN issue for clear, concise analysis and efficient troubleshooting.

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

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



11:54:23 AM

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

1. Devices / Firewalls Involved:

- FGTs: office

2. Impacted SD-WAN Interfaces and Associated Issues:

- exit-int-2
 - Issue: External Server Issue
 - Impacted Clients:
 - IND-PR8
 - IND-ARF
 - IND-34S
 - IND-C34
 - IND-2QR
 - etc.
 - Health Checks Impacted: wan_ping_sla
- exit-int-1
 - Issue: ISP or Server Performance Deviations
 - Impacted Clients:
 - IND-PR8
 - IND-2QR
 - IND-NAI
 - IND-MM
 - IND-4C9
 - etc.
 - Health Checks Impacted: wan_ping_sla

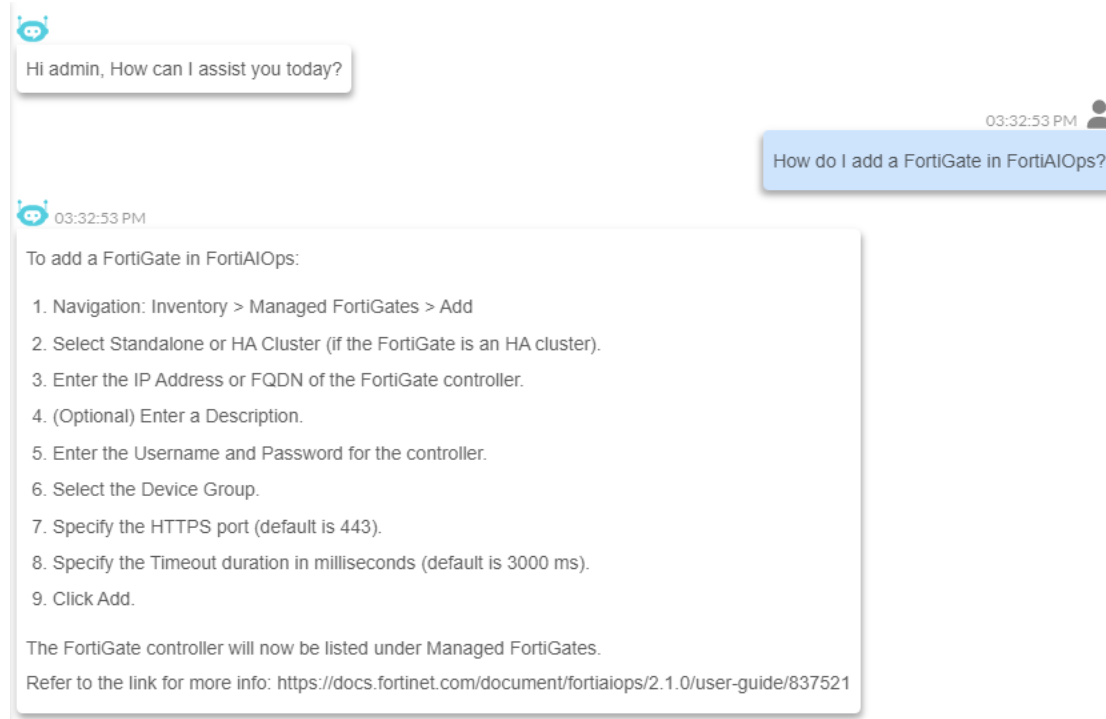
3. Clients Affected (Grouped and Deduplicated):

- IND-PRE
- IND-ARPI
- IND-34SX
- IND-C348
- IND-2QR0
- IND-NAIR
- IND-MMU
- IND-4C9Z
- etc.

Example 5: Assistance with Device Setup

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

Prompt: How do I add a FortiGate in FortiAI Ops?



Example 6: Tabular Format Display

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

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

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

11:48:03 AM

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

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

Key Points:

- Wireless authentication failed due to RADIUS misconfiguration or invalid credentials on device 6.83x-3F-[REDACTED]
- Wired issues on device 3FHR-[REDACTED] (Switch S224DF3X1 [REDACTED]): high CPU and memory usage, and elevated device temperature.
- Recommended actions include verifying credentials, checking for high resource utilization causes, and reviewing hardware cooling and alert thresholds.

Device Details:

- 6.83x-3F-[REDACTED] (Wireless)
- 3FHR-[REDACTED] Switch S224DF3X1 [REDACTED] (Wired)

If further details are needed, please specify.

Example 7: Analyze PCAP file

You can upload existing PCAP files for AI analysis. Once uploaded, you can ask questions regarding the traffic, such as identifying DHCP issues, troubleshooting connectivity for specific client MAC addresses, counting probe requests, and so on.

Prompt: Analyze the uploaded packet capture file: <file_name>



Hi admin, How can I assist you today?

02:38:45 PM

Analyze the uploaded packet capture file: dhcp_test.pcap



02:38:45 PM

Key Observations

- **High proportion of TCP traffic (247 frames) compared to UDP (28 frames), with most TCP frames associated with a protocol labeled "dhcpfo".**
-> Indicates the network is primarily using TCP-based communication, and "dhcpfo" may be a custom or misidentified protocol layered over TCP.
- **DHCP traffic is present but limited to 28 UDP frames, totaling 11,770 bytes.**
-> Suggests DHCP activity is occurring, but is not the dominant traffic type in this capture.
- **Top talkers include several non-standard or malformed IP addresses (e.g., 192.168.1.255.255).**
-> Implies possible data obfuscation, anonymization, or errors in IP address parsing within the capture.
- **Protocol hierarchy shows deep nesting of "dhcpfo" frames, with repeated encapsulation.**
-> May indicate tunneling, protocol misidentification, or unusual application behavior that warrants further investigation.

If you'd like deeper analysis, try asking questions specific to this DHCP capture (for example: "Are there signs of DHCP spoofing?", "What devices are requesting IP addresses?", "Is there evidence of DHCP starvation or flooding?").

02:39:07 PM

are there any dhcp issues in the capture



02:39:07 PM

The packet summaries show normal DHCP operations with no clear evidence of failed handshakes, missing offers, starvation, spoofing, or abnormal message patterns.

Analysis:

- The capture includes complete DHCP handshakes: Discover, Offer, Request, and ACK sequences are present for the observed MAC addresses and transaction IDs.
- DHCP Inform messages are seen repeatedly, which is normal for clients seeking additional configuration.
- There are no signs of DHCP starvation (no excessive Discover/Request without Offers/ACKs), nor evidence of spoofing (all DHCP messages appear to originate from expected sources).
- No missing DHCP Offers or failed handshakes; every Request is followed by an ACK.
- The packet count is 28, covering several full DHCP cycles and release events.

Additional Insights

1. Notable pattern: The same MAC addresses and transaction IDs are used consistently, and all expected DHCP message types are present in proper order.
2. No anomalies such as repeated failed Requests, missing Offers, or excessive Discover messages.
3. Total matching packets: 28.

Would you like me to... review the timing between DHCP messages for performance issues, or check for unusual DHCP option usage?

02:42:26 PM

may i know which client requesting ip in the capture and what ip?

02:42:26 PM

The packet summaries show that the DHCP client with MAC address 00:0c:29:42:7a is requesting an IP address in the capture.

- The specific IP address requested by this client is 192.168.1.10 (as seen in the DHCP Request and DHCP Discover packets).

Additional Insights

1. Only one DHCP client (MAC: 00:0c:29:42:7a) is actively requesting an IP address in the capture.
2. The requested IP address (192.168.1.10) is not a valid IPv4 address format, which may indicate obfuscation, anonymization, or a parsing issue in the capture.
3. The DHCP handshake sequence (Discover, Offer, Request, ACK) is present for this client, confirming normal DHCP operation.
4. Total matching DHCP request packets with requested IP: 2 (plus additional requests without explicit requested IP).

Would you like me to... check for other DHCP clients, analyze the DHCP lease process in detail, or investigate why the requested IP address appears invalid?

02:43:31 PM

may i get transaction id for those

02:43:31 PM

The packet summaries show several DHCP transactions with distinct transaction IDs for clients requesting IP addresses.

Response to your query:

The DHCP transaction IDs for clients requesting IP addresses in the capture are:

- 0x8b1967 (seen in DHCP Discover, Offer, Request, ACK, and subsequent Requests/ACKs)
- 0xc6e (seen in DHCP Discover, Offer, Request, ACK, and subsequent Requests/ACKs)

Additional Insights

1. There are two main DHCP transaction IDs associated with full DHCP handshakes (Discover, Offer, Request, ACK), indicating two separate DHCP lease cycles.
2. Other transaction IDs (e.g., 0x29b6e1d48) are only seen in DHCP Inform messages, not in IP address requests.
3. DHCP Release messages use transaction IDs 0xd14114da7424, indicating lease releases.
4. Total matching packets: 28, with multiple packets for each transaction ID.

Would you like me to... identify the exact timestamps or sequence of each DHCP transaction, or correlate these transaction IDs with client MAC addresses for deeper analysis?

Example 8: Trigger Packet Capture

You can initiate a packet capture on a specific FortiGate interface. The PCAP file thus generated can be downloaded for further analysis.

Prompt: trigger packet capture on <interface name> at <FGT name>

01:02:01 PM

trigger packet capture on port4 interface at FG10157103000153 FGT

01:02:01 PM

Key Observations

- **TCP is the dominant protocol, with all 147 frames using TCP over IP and Ethernet.**
-> Indicates the traffic is primarily connection-oriented and reliable, typical for application-level communications.
- **TLS traffic is present (13 frames, 1872 bytes), alongside RSH, MSDO, and generic data.**
-> Suggests encrypted sessions are active, but also legacy/less secure protocols (RSH) and possible proprietary or miscellaneous data.
- **RSH protocol detected (1 frame, 158 bytes).**
-> Use of RSH is a security concern, as it transmits data unencrypted and is considered obsolete.
- **Top talkers are internal IPs (21.43.x.x), with relatively low byte counts per flow.**
-> Implies either short-lived connections or low-volume data exchanges, possibly control or signaling traffic.

 If you'd like deeper analysis, try asking questions specific to this wired capture (for example: "Are there signs of suspicious activity on port4?" or "Which applications are using TLS on this segment?").

 [Download the packet capture file](#)

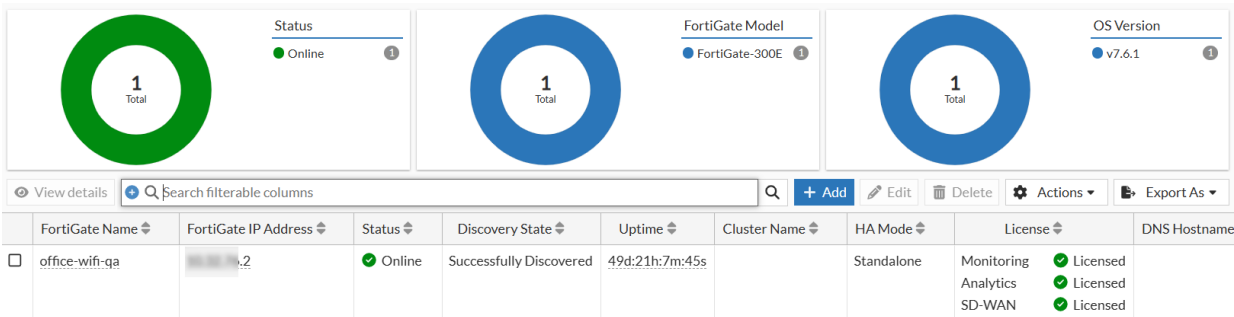
Inventory

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

- [Adding and Managing FortiGates](#)
- [ADOMs](#)
- [VDOM Support](#)

Adding and Managing FortiGates

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



You can perform the following operations on this page.

- [Adding a FortiGate](#)
- [Importing and Exporting FortiGates](#)
- [Managing FortiGates](#)

Adding a FortiGate

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

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

- If the FortiGate IP address is configured in FortiAIOps then the SAN attribute in the certificate should be the FortiGate IP address.
- If the FortiGate FQDN is configured in FortiAIOps then the SAN attribute in 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

Description

Username

Password

Confirm Password

ADOM

Default
▼

HTTPS port

443

Timeout (milliseconds)

5000

Add

Cancel

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 **ADOM**. Controllers in the selected ADOM are added.
5. Specify the **HTTPS port**. The default is 443.
6. Specify the **Timeout** duration (milliseconds), that is, the maximum time allowed to establish a connection with FortiGate and obtain a response. The default value is 5000 milliseconds.

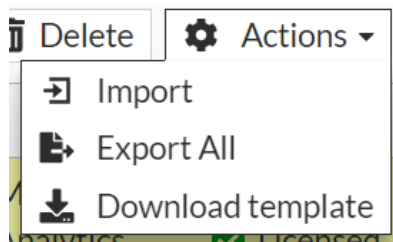
The added FortiGate controller is now listed.

Importing and Exporting FortiGates

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

	A	B	C	D	E	F	G	H
1	Device Type	IP address	Description	Username	Password	Device Group	HTTPS port	Timeout (milliseconds)
2	Standalone	10.20.100.20	fortigate1	admin	fortigate1	guestgroup	443	3000
3	Standalone	10.20.100.20	fortigate2	admin	fortigate2	test2	10443	3000
4	Standalone	10.20.100.20	fortigate3	admin	fortigate3	guestgroup	443	3000

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



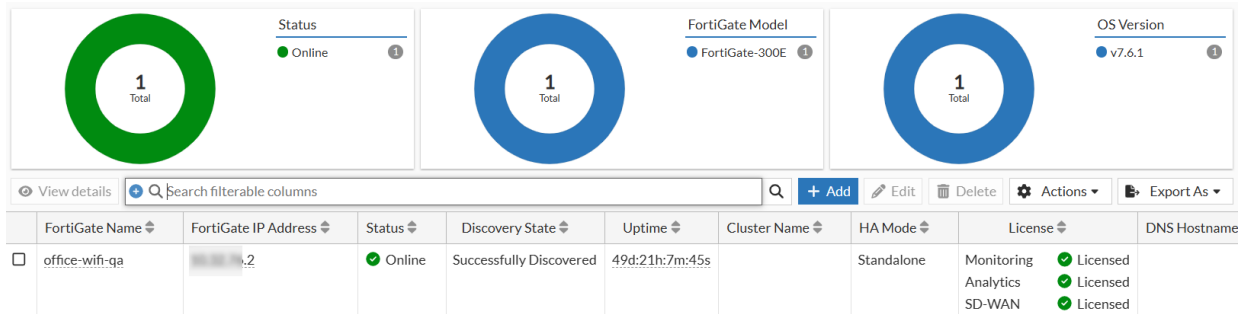
Select **Import** to upload the FortiGate configuration file.

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

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

Managing FortiGates

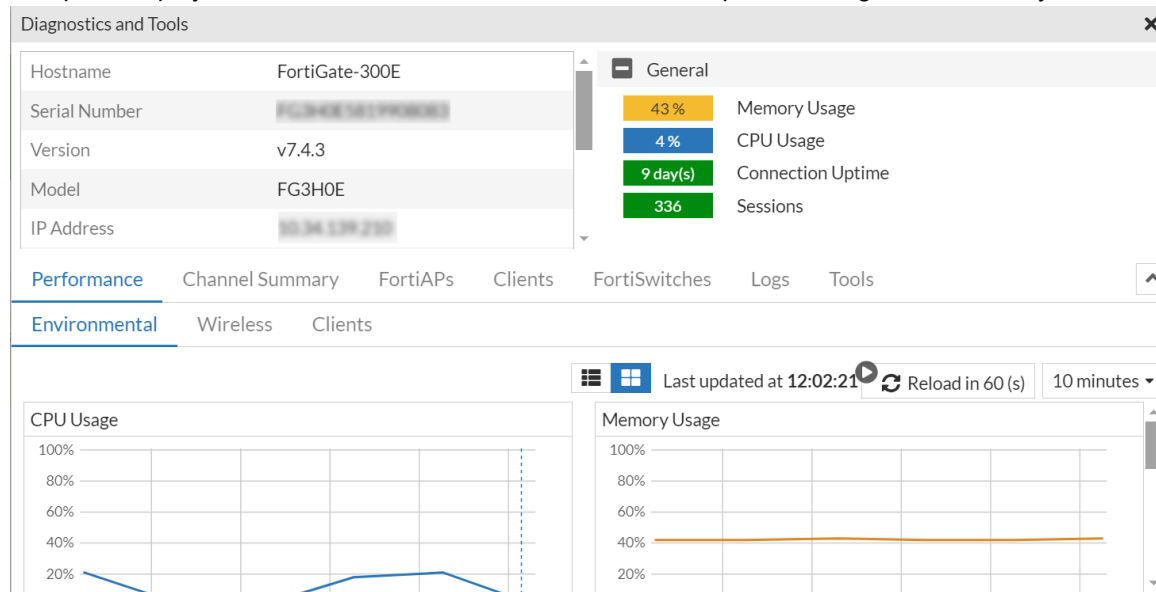
This page provides analytical information related to the performance of various elements and processes in your network. The data is visually represented with interactive options to drill-down and filter specific information. This enables monitoring, diagnostic, and troubleshooting operations for connectivity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



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

- **Add** - Select to add a FortiGate controller manually. For more information, see [Adding a FortiGate](#).
- **Actions** - Click **Actions** to import and to download the template.
- **Export As** - Click to export the table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.
Note: You customize your exports by choosing which columns to be included in the export. A maximum of 8 columns can be selected.
- **View Details** - Select a FortiGate and click **View details** to open **Diagnostics and Tools** pane. You can also right-click the FortiGate and click **View details**.

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



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

Performance

This tab displays the performance data for your network based on various parameters. You can filter the trends based on the selected duration or customized time slot; select a time window or define a Custom range. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**. The data in this tab is automatically refreshed every 60 seconds; the following options are available to manage the auto-refresh feature for this page.

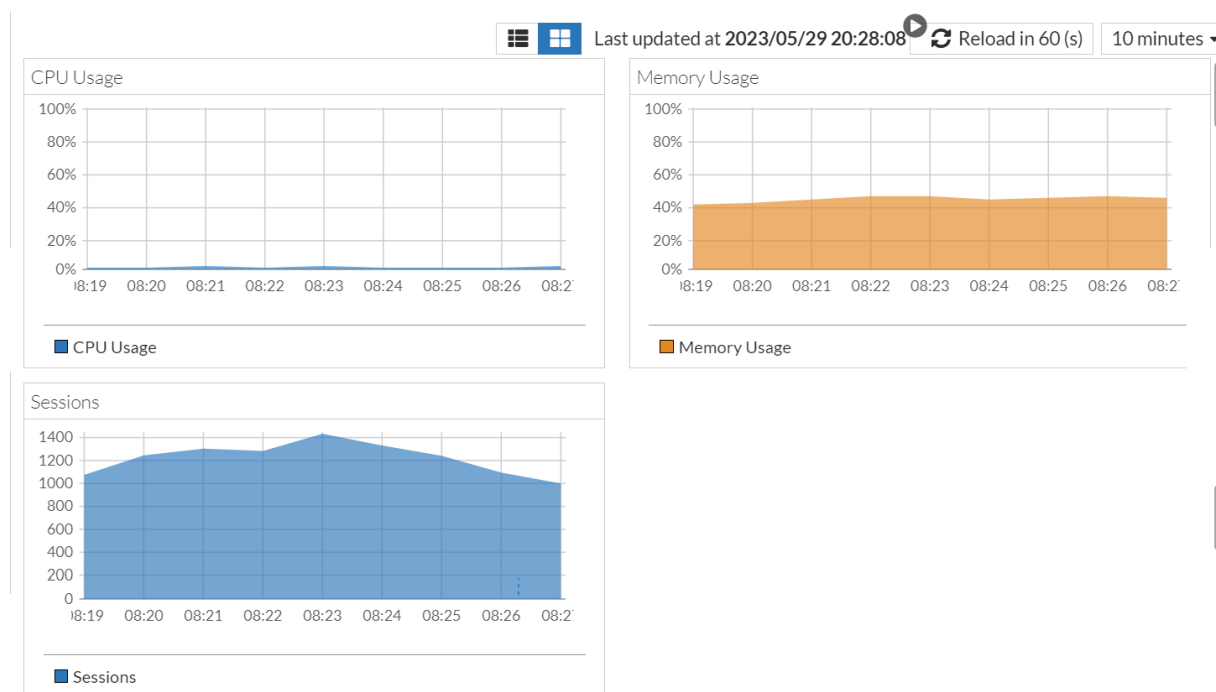
- Click  to manually refresh data.
- Click  to pause the auto-refresh.
- Click  to resume the auto-refresh.

Performance is displayed for the following.

- [Environmental](#)
- [Wireless](#)
- [Clients](#)

Environmental

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

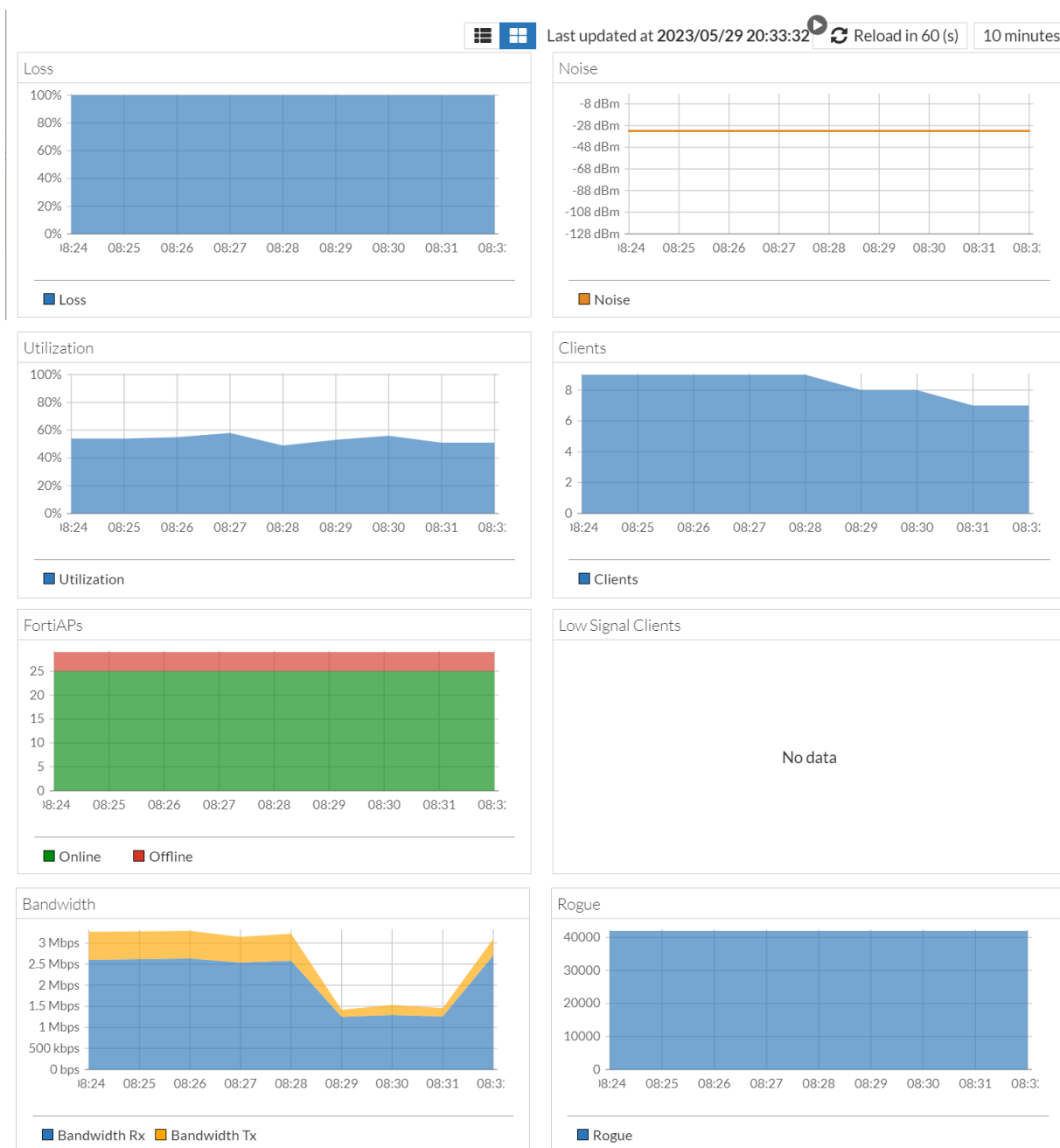


Hover over each of these graphs to view the current statistics and click on any of these graphs to view details.

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

Wireless

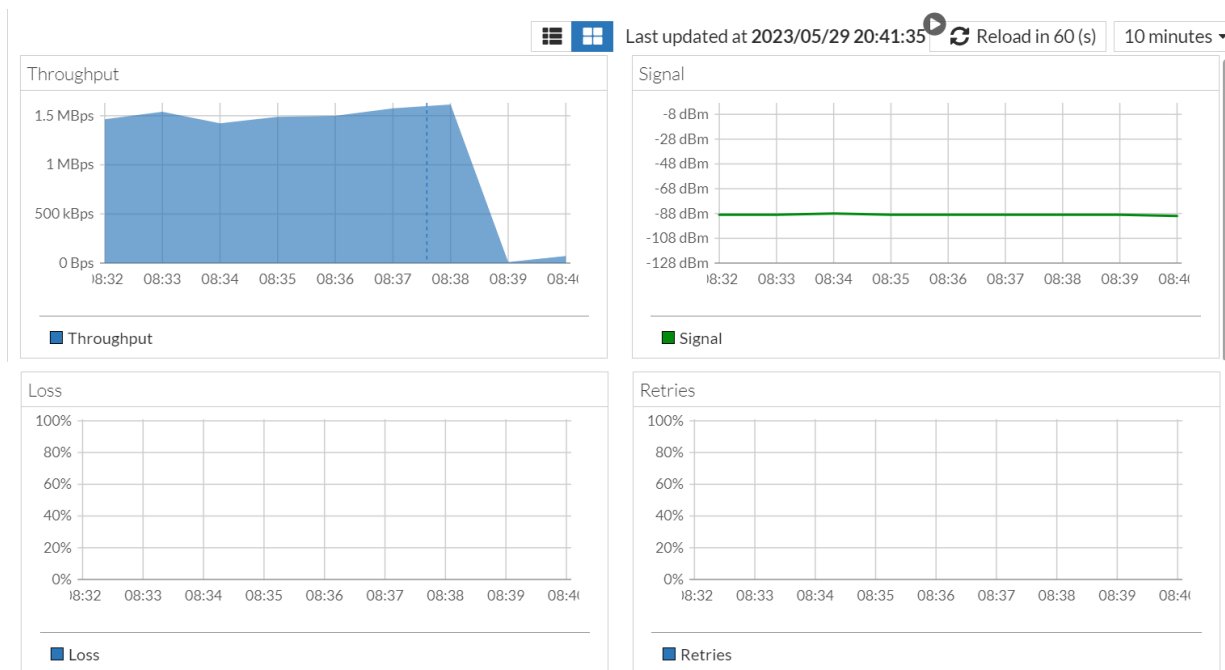
Displays detailed information about the health of the wireless connections in the network, such as, loss%, SNR, channel utilization %, number of stations, status of the FortiAPs, low signal stations, the average throughput at a given time, and the number of rogue APs at a given time.



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

Clients

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



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

Channel Summary

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

View details Trends Search filterable columns C					
Channel ▾	Max Channel Utilization ▾	Clients ▾	No. Of Radios ▾	Average Utilization Severity ▾	Average Interfering SS
2.4 GHz 3 Number of Clients-0					
1	90 %	0	5	Poor	Good
11	97 %	0	4	Poor	Good

FortiAPs

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

Clients

This tab displays the clients currently connected to the selected access point along with their details. To view the details, select a client and click **View Details**. For more information on the diagnostic options and details see [Wireless Clients on page 201](#).

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](#).

Ports						
Cable Test						
Logs						
Statistics						
Clients						
+ Search						
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.

Performance						
FortiAPs						
Clients						
FortiSwitch						
Logs						
Tools						
+ Search						
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.

Performance						
FortiAPs						
Clients						
FortiSwitch						
Logs						
Tools						
+ Search						
Date/Time	Level	Action	Message	Details		
2 minutes ago		rogue-ap-detected	AP OnePlus 7	General Source Action Security Cellular Event		
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

Maximum captured packets ☒

☒ Filters

Filtering syntax **Basic** Advanced

Host

+

Port

+

Protocol

+

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

+

Q

Search

Q

Source IP	Source Port	Destination IP	Destination Port	Protocol	Sequence Number	Ack
172.16.200.254	57224	172.16.200.1	443	TCP	1964315332	3719362240
172.16.200.254	57194	172.16.200.1	443	TCP	1964315332	3371865
172.16.200.254	57194	172.16.200.1	443	TCP	1964315332	3371865

0% 10

Header

Packet Data

IP		L4	
Source IP	172.16.200.254	Ack	3719362240
Source Port	57224	Flags	ACK
Destination IP	172.16.200.1	Window	41488
Destination Port	443	Length	0
Protocol	TCP	Checksum	26989

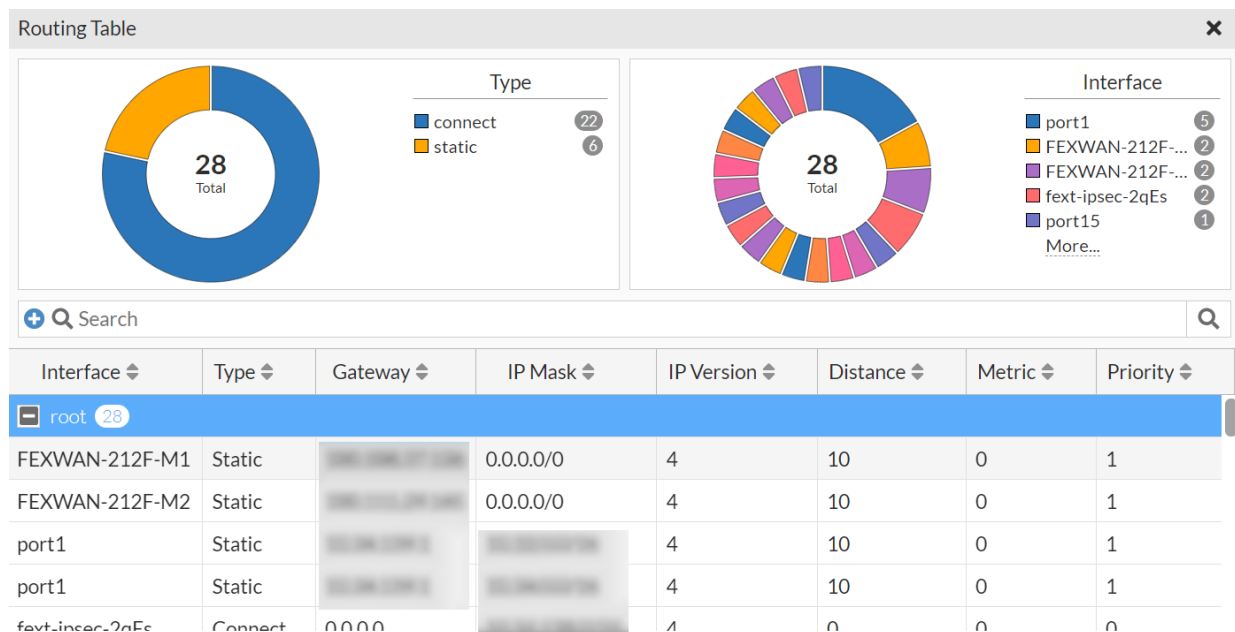
ARP Table

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			
+ Q Search Q			
Age	Interface	IP	MAC Address
root 4			
1m 24s	wan1	172.16.200.1	172.16.200.1
1s	25SSID-Coverage	172.16.200.1	172.16.200.1
0s	wan1	172.16.200.1	172.16.200.1
15s	wan1	172.16.200.1	172.16.200.1

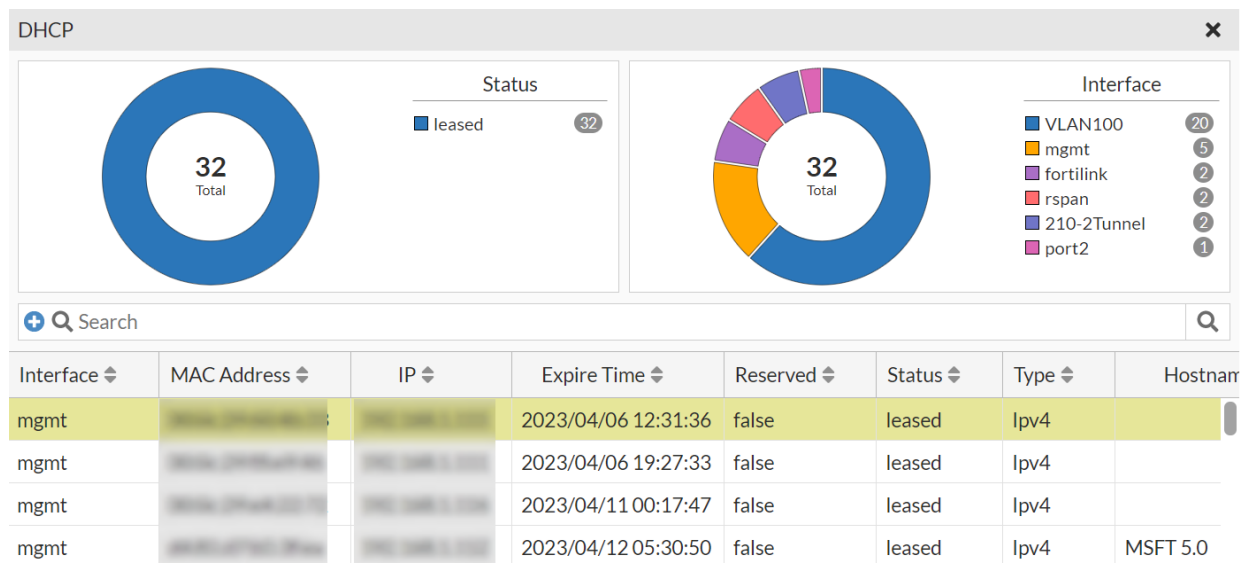
Routing Table

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



DHCP

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



DNS Lookup

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

DNS Lookup

FQDN

IP Address

Reverse DNS Lookup

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

Reverse DNS Lookup

IP Address

FQDN

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**.

TAC Report



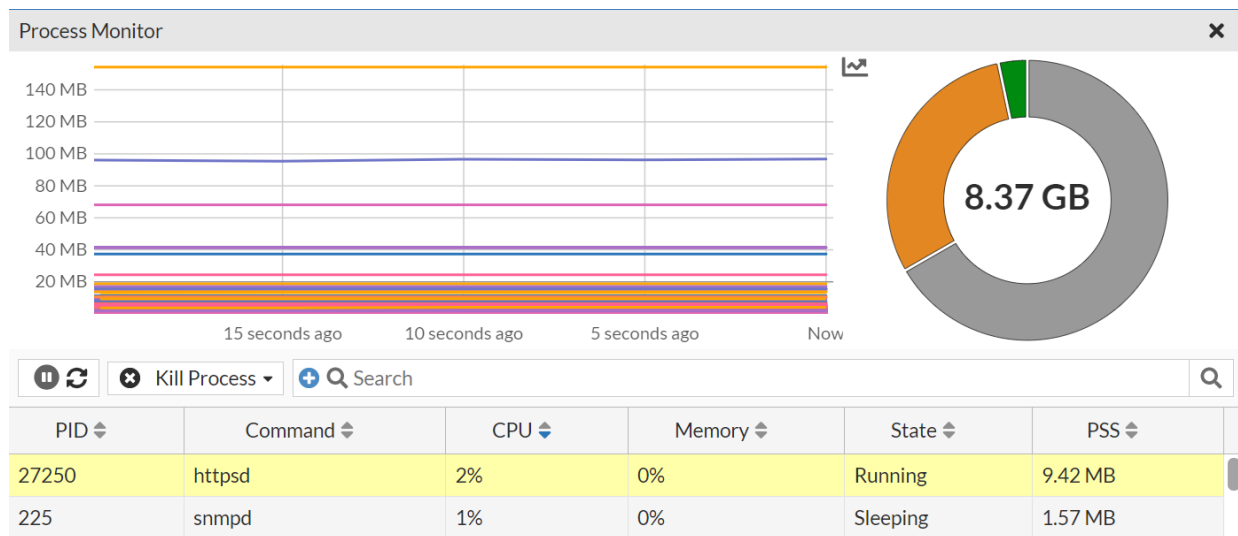
Report generated



Download report

Process Monitor

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



Select a process to perform any of the following operations.

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

For more information on the FortiGate commands and related information, see [FortiGate documentation](#).

ADOMs

You can group FortiGate controllers for ease of management. Each controller can belong to only one ADOM; if a controller is added to a second ADOM, it is automatically removed from the previous ADOM. ADOMs 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 ADOMs and devices within them. System administrators and users assigned the *super user* role can only create and configure ADOMs.

Dashboard	>	+ Add Edit Delete Search	
AI Insights	>		
Inventory	>		
Managed FortiGates	>		
ADOMs	>		
Wireless	>		
Switch	>		

	ADOM Name	Description
☐	Default	Default Device group
☐	Pine Corp	
☐	401.20.0.0/24 Corp	
☐	192.168.0.0/24 Corp	

If you do not set up ADOMs, all controllers remain assigned to the *Default* ADOM.

1. Navigate to **ADOMs** and click **Add**.

Add new ADOM

Details

ADOM Name

Description

Devices

+ 🔍 Search filterable columns

	FortiGate Name ▾	FortiGate IP Address ▾	ADOM ▾	Status ▾	Serial Number ▾	OS Version ▾
☐	HA Backup_2	10.34.136.222	Default	🟢 Online	FGT140C7K130P088JD	v7.0.12
☐	FGT_PRIMARY_181	10.34.136.181	2	🔴 Offline	FGVM02TM25002356	v7.6.0
☐	ofice-with-g	10.32.76.2	3rd_BLR_Corp	🟢 Online	FGS140C7K130P088J81	v7.6.1
☐	Pune-Office-WiFi1	10.32.127.222	Pune_FGT	🟢 Online	FG2140C7K130P088J23	v7.6.4
☐	vinod-fgt	10.34.152.212	test	🟢 Online	FGVM04TM25002851	v7.6.4

Add

Cancel

2. Provide a unique **ADOM Name** and an optional **Description**.
3. A list of controllers managed by FortiAI Ops is displayed. Select from the listed controllers and click **Create**. The controllers are added to the ADOM.

You can switch the ADOM from the bar on the top-right of the GUI; click **ADOM** and select the available group. To add a FortiGate controller to an existing ADOM or move a FortiGate to a different ADOM, select the ADOM 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 ADOM and click **Update**.

VDOM Support

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

Adding/Managing VDOMs in FortiAI Ops

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

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

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

- Wireless > Access Points

	AP Name	FortiGate	AP Status	VDOM	SSID	Band	Channel	Clients
☐	FP431GT	office-wifi-qa	Online	root	R2 JK_TEST_CORP R3 None	R2 5 GHz R3 6 GHz	R2 36 R3 N/A	6
☐	83x_3F	office-wifi-qa	Online	root	R1 Corp_FortiPresence_PSK R2 Corp_FortiPresence_PSK	R1 2.4 GHz R2 5 GHz	R1 11 R2 44	0
☐	3.83x-3F	office-wifi-qa	Online	root	R2 Corp-Fortiguest-CP-3F_2,Forti-Corp-Peap-3F,F...	R2 5 GHz	R2 44	4

- Wireless > Clients

	MAC Address	FortiGate	IP Address	AP Name	AP Serialnumber	VDOM	SSID	Device
☒	F8:E4:E3:	FG3H0E	192.168.1.1	5.83x-3F	FP831FTF	root	Corp-Fortiguest-CP-3F	IND-9H3
☐	F8:5E:A0:	FG3H0E	10.32.1.1	1.83x-3F	FP831FTF	root	Corp_AIOPs_test	IND-JKIN
☐	F0:D4:15:	FG3H0E	10.32.1.1	3.83x-3F	FP831FTF	root	Forti-Corp-Peap-3F	IND-F19
☐	F0:D4:15:	FG3H0E	10.32.1.1	7.83x-3F	FP831FTF	root	Corp_AIOPs_test	DESKTOP

- Switch > FortiSwitch

	Name	FortiSwitch Serial Number	FortiGate	Status	Model	VDOM	Firmware Version	Connecting From
☒	3FHR-AP-SW1	S224DF3X	office-wifi-qa	Online	S224DF	root	S224DF-v7.4.0-build767,230602 (GA)	10.32.1.1
☐	GFHR-AP-SW1	S248DF3X	office-wifi-qa	Online	S248DF	root	S248DF-v3.6.12-build436,230614 (GA)	10.32.1.1
☐	2FSR-AP-SW1	S548DF50	office-wifi-qa	Online	S548DF	root	S548DF-v7.4.0-build767,230602 (GA)	10.32.1.1

- Switch > FortiSwitch Clients

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

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

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

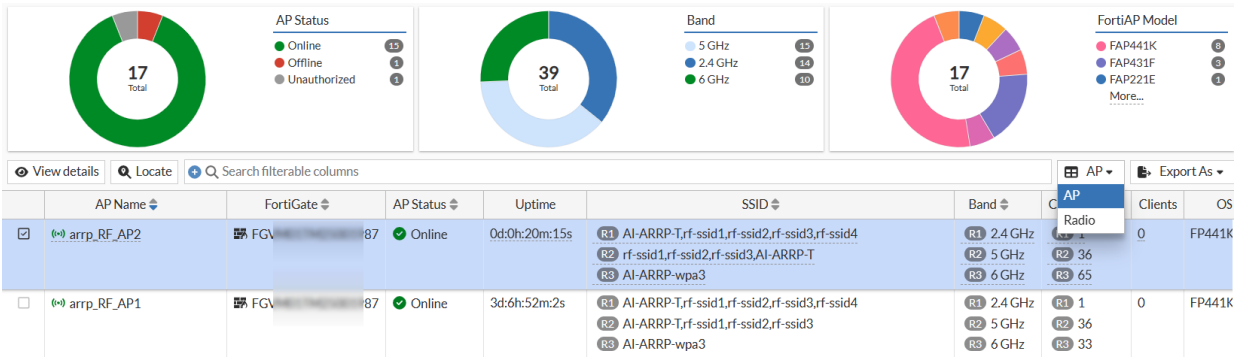
Wireless

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

- [Access Points](#)
- [Wireless Clients](#)
- [Channel Summary](#)
- [AI-ARRP](#)
- [Applications](#)
- [Rogue APs](#)
- [Wi-Fi Maps](#)

Access Points

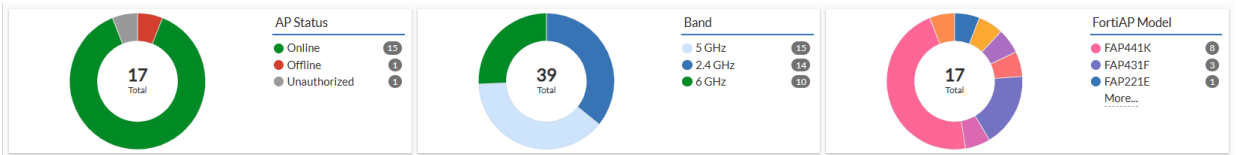
The Access Points page displays essential information about the APs in use and consists of two views - AP and Radio view. To switch between the AP and Radio views, select the desired view from the dropdown menu located at the middle of the Access Points page. By default, the AP is displayed when the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



- [AP](#)
- [Radio](#)
- [Diagnostics and Tools](#)

AP

The AP view displays information related to the Access Point and consists of three widgets - FortiAP status, number of APs in each band, and FortiAP model details.



FortiAP Status

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

Band

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

FortiAP Model

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

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

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

You can find the physical location of an AP using the Locate button. Select an AP and click **Locate**. The system opens the **Wi-Fi Maps** window to highlight the placement of the selected AP on its floor plan. For more information, see [Locating Wireless Devices on the Map](#).

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.

The screenshot shows the FortiAP Status page with three donut charts at the top: AP Status (17 Online, 1 Offline, 1 Unauthorized), Band (39 Total: 15 5 GHz, 14 2.4 GHz, 10 6 GHz), and FortiAP Model (17 Total: 10 FAP441K, 4 FAP431F, 3 FAP221F). Below the charts is a table of APs. A 'Select Columns' dialog is open, showing a list of columns to be added to the table. The dialog has a search bar and two columns: 'Active Columns' (Total: 14) and 'Inactive Columns' (Total: 6). The 'Active Columns' list includes AP Name, FortiGate, AP Status, Uptime, SSID, Band, Channel, Clients, OS Version, LLDP, FortiAP profile, VDOM, Connected via, and License. The 'Inactive Columns' list includes AP Serial Number, Channel Utilization, FortiAP Model, FortiGate IP Address, FortiGate Serial Number, and MAC Address. The 'Apply' button is at the bottom right of the dialog.

AP Name	FortiGate	AP Status	Uptime	SSID
arrp_RF_AP2	FGV100F01987	Online	0d:0h:35m:5s	R1 AI-ARRP-T,rf-ssid1,rf-ssid2,rf-ssid3 R2 rf-ssid1,rf-ssid2,rf-ssid3 R3 AI-ARRP-wpa3
arrp_RF_AP1	FGV100F01987	Online	3d:7h:6m:52s	R1 AI-ARRP-T,rf-ssid1,rf-ssid2,rf-ssid3 R2 AI-ARRP-T,rf-ssid1,rf-ssid2,rf-ssid3 R3 AI-ARRP-wpa3
desk_231G_arrp	FGV100F01987	Online	3d:7h:6m:12s	R1 AI-ARRP-T,Garrp1 R2 AI-ARRP-T,Garrp2 R3 AI-ARRP-wpa3
desk_431F_arrp	FGV100F01987	Online	3d:7h:6m:50s	R1 AI-ARRP-T,rf-ssid1,rf-ssid2,rf-ssid3 R2 AI-ARRP-T,rf-ssid1,rf-ssid2,rf-ssid3 R3 AI-ARRP-wpa3
desk_243K_arrp	FGV100F01987	Online	3d:7h:6m:28s	R1 AI-ARRP-T,Karrp1 R2 1_Location_Test,AI-ARRP-T,Karrp2 R3 1_6E_205,AI-ARRP-T,Karrp2
Desk_441_arrp	FGV100F01987	Online	3d:7h:5m:59s	R1 AI-ARRP-T,Karrp1 R2 AI-ARRP-T,Karrp2 R3 1_6E_205,AI-ARRP-T,Karrp2

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

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

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

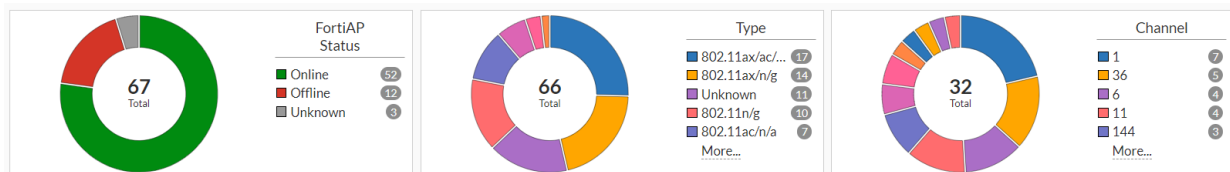
Click the plus icon located to the left of the search bar to perform a more specific search based on a particular column. Select the desired column, and then enter the search term to narrow down the search results to specific criteria.

Click **Export As** to export the table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.

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

Radio

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



Status

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

Type

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

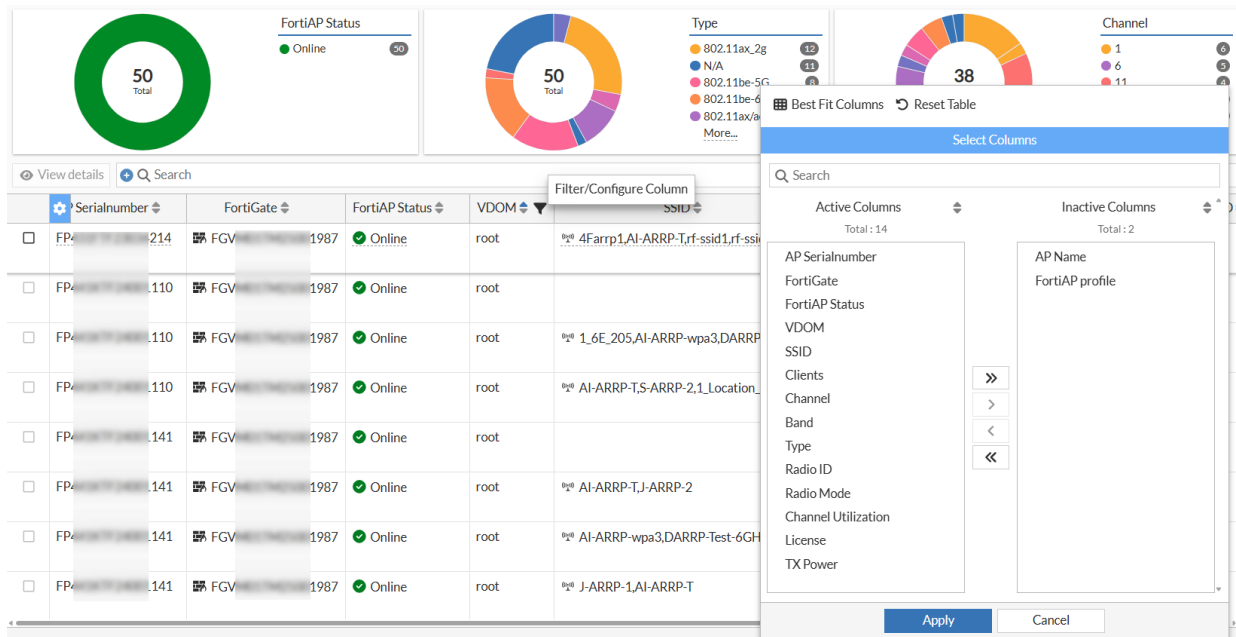
Channel

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

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

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

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



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

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

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

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

Click **Export As** to export the table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.

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

Access Points Diagnostics and Tools

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

Locate

The **Locate** button is available in the **Diagnostics and Tools** pane for the **AP** view. Click **Locate** to find the physical location of an AP. The system opens the **Wi-Fi Maps** window to highlight the placement of the selected AP on its floor plan. For more information, see [Locating Wireless Devices on the Map](#).

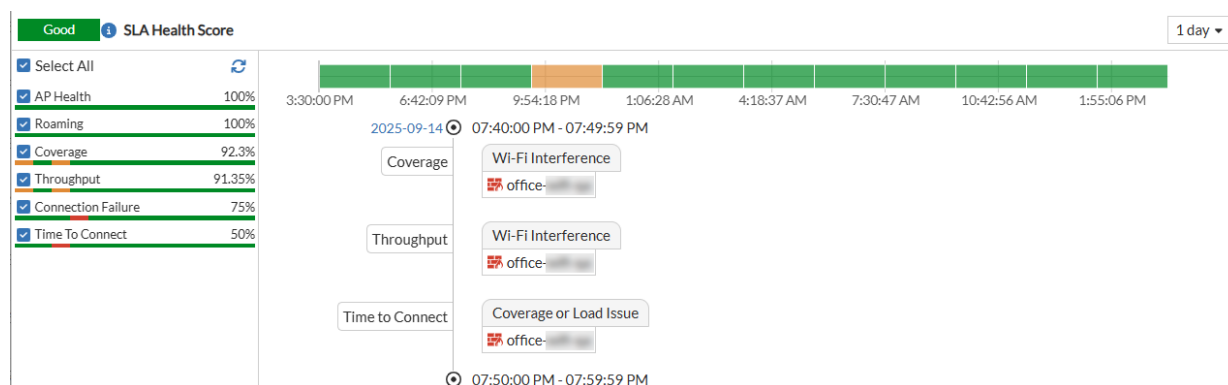
The following tabs are available:

- [AI Insights](#)
- [Performance](#)

- [Channel Summary](#)
- [Clients](#)
- [Interfering SSIDs](#)
- [Logs](#)
- [Spectrum Analysis](#)
- [VLAN Probe](#)

AI Insights

The **AI Insights** tab helps to analyze various performance metrics, identify issues, and provide detailed insights into the root cause of network problems, helping administrators maintain high service levels.



Note: This feature may not work as expected on Safari browser. For the best experience, use Chrome, Firefox, or Microsoft Edge instead.

The **SLA Health Score** provides the overall high-level score.

- **Good** for a score more 70
- **Fair** for a score between 30 and 70
- **Bad** for a score less than 30

Below the overall score, a list of individual SLAs or metrics is shown with their current health scores. You can select the SLAs that you want to track.

The following metrics are available:

- AP Health
- Roaming
- Coverage
- Throughput
- Connection Failure
- Time To Connect

When you click an SLA, the corresponding **SLA Summary** window opens with more details.

The bar graph shows the performance trend over a selected time period (in this case, 1 day). The graph is divided to equal time segments. Based on the health score of each segment, the segments are colour coded as green (good), orange (fair), and red (bad).

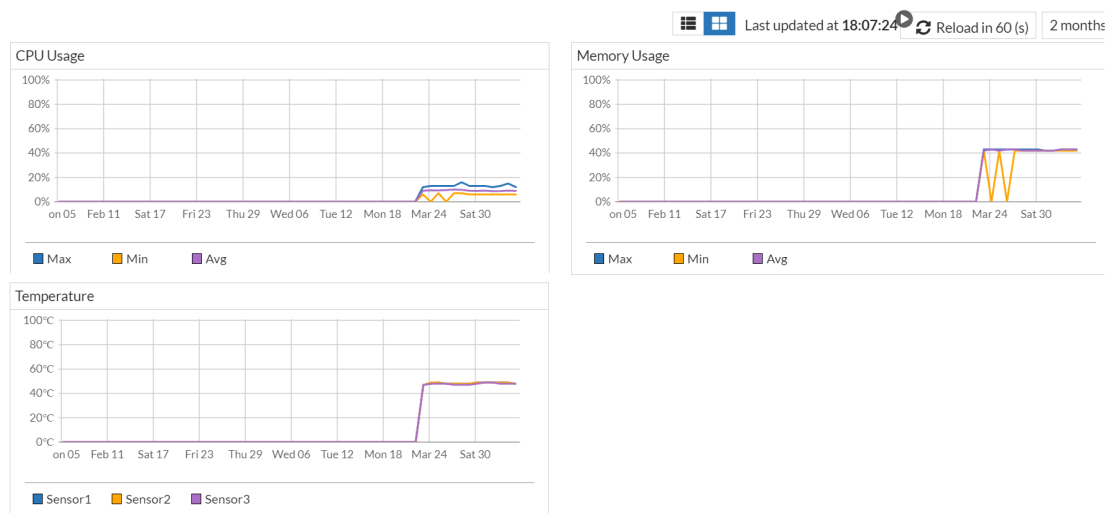
Clicking on a specific time segment displays more details events that occurred during the time period.

Performance

The performance tab displays trends for the FortiAP health, wireless, and wired clients for selected interval. You can filter the trends based on the selected duration or customized time slot; select a time window or define a custom range. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**. The minimum, maximum, and average values are displayed when a time interval of more than 6 hours is selected.

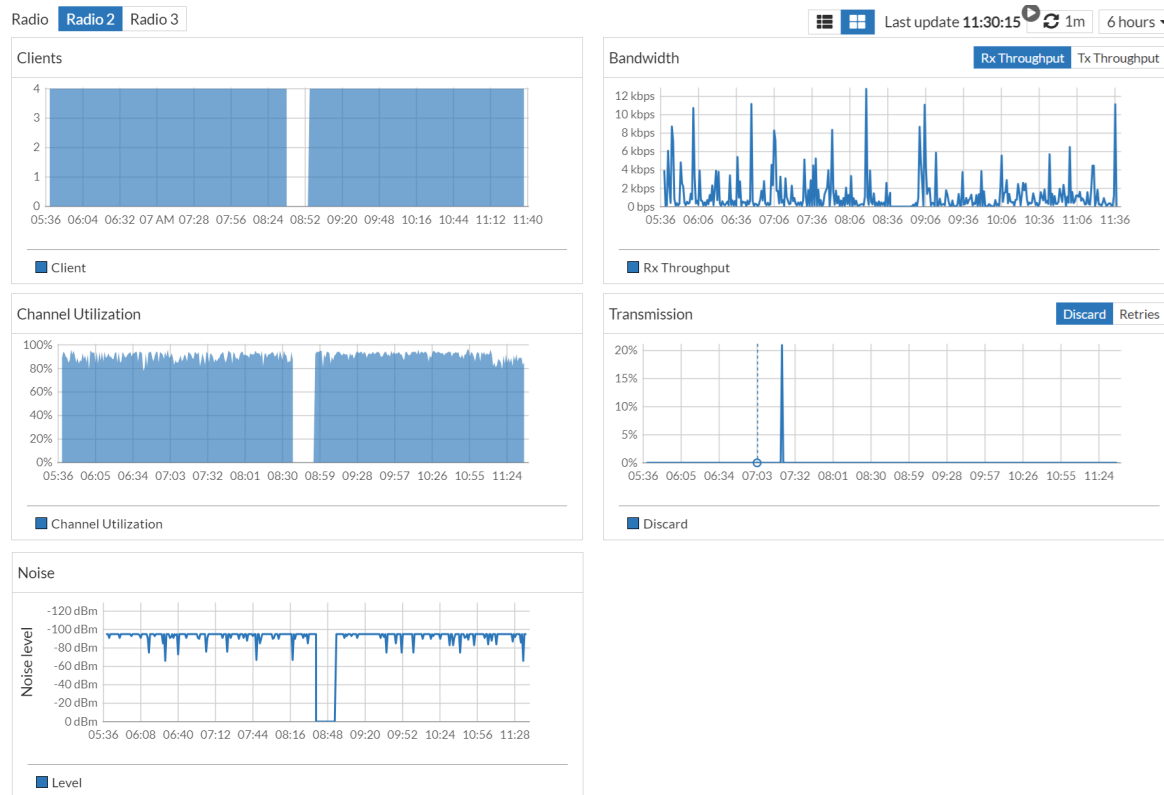
AP Health

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

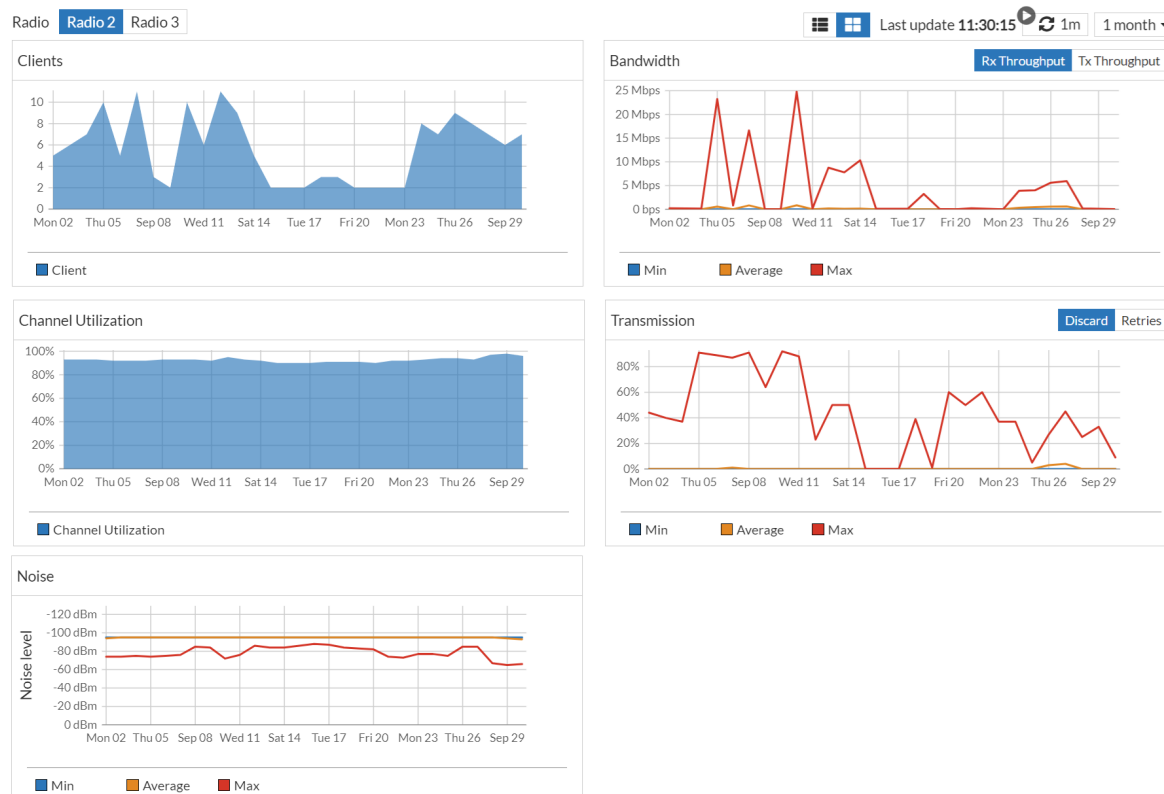


Wireless

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



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



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

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

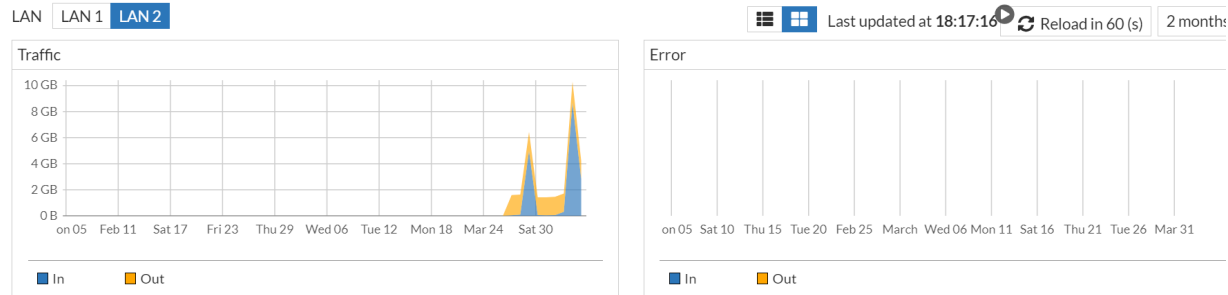
The following image depicts the details displayed for an interval of more than 6 hours.

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

Wired

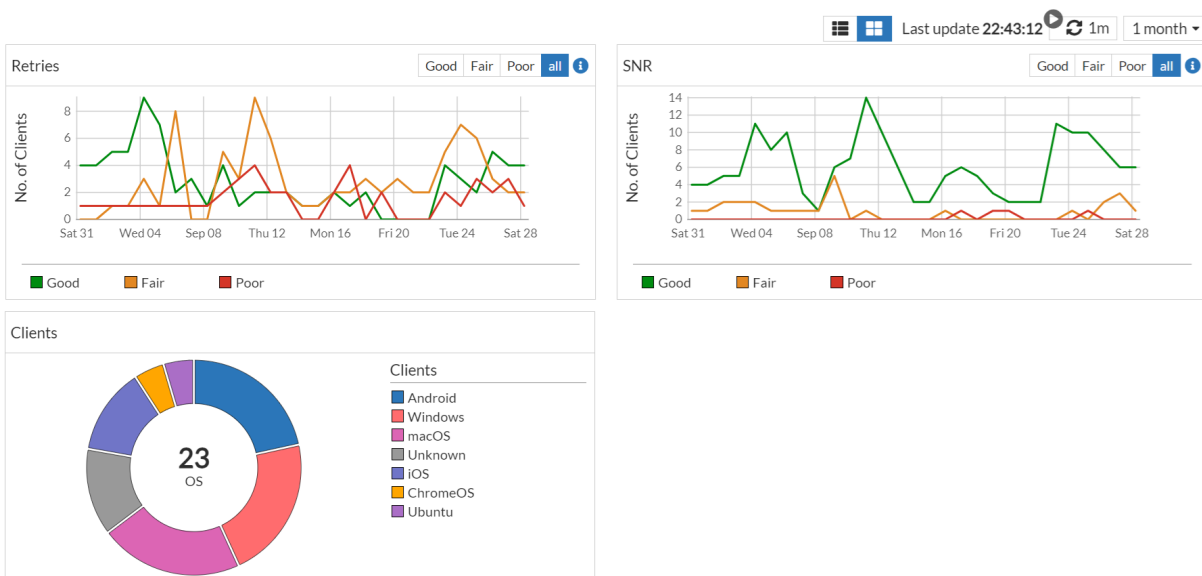
The LAN port statistics are now displayed for access points. You can view the traffic coming into a LAN port and the traffic leaving it at a given point in time. Also, the error statistics for both incoming and outgoing traffic is displayed.

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



Clients

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



- [Retries](#)
- [SNR](#)
- [Clients](#)

Retries

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

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

SNR

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

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

Clients

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

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

Details

Search filterable columns

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

Channel Summary

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

View details

Trends

Search filterable columns

C

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

Clients

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

View details

Search

MAC Address	FortiGate	IP Address	Forti AP	SSID	Device	User	Channel	Band
	FortiGate-300E			210-2Tunnel	FTNT-THINK-2		132	18.27
	FortiGate-300E			210-Bridge	FortiAlsQAsMini		132	0

Interfering SSIDs

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

SSID	AP BSSID	Channel	Signal	Type
Radio Id: 1 156				
1A_no_vlan		11	-27 dBm	Other
#####iperf_SSID		11	-61 dBm	Other
test		11	-51 dBm	Other
test		11	-64 dBm	Other

Logs

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

Search filterable columns				Q	Details
Date/Time	Level	Action	Message	General	
2024/04/12 21:...		auth-req	AP received auth	Absolute Date/Time 2024/04/12 21:11:47	
2024/04/12 21:...		auth-req	AP received auth	Time 21:11:47	
2024/04/12 21:...		auth-req	AP received auth	Virtual Domain root	
2024/04/12 21:...		auth-req	AP received auth	Log Description Authentication request from wireless station	

Spectrum Analysis

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

Notes:

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

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

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

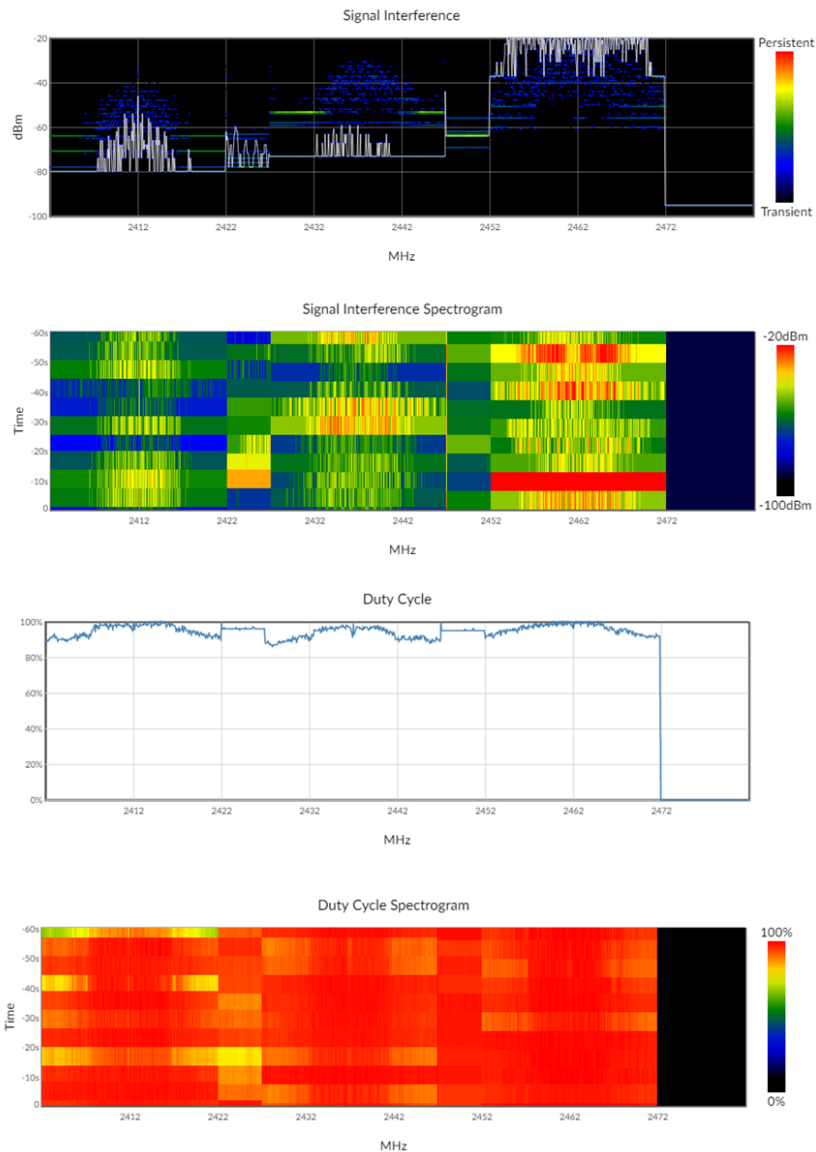
Select **Start** and the GUI periodically polls the spectrum analysis data based on the fixed sampling interval of 1000 milliseconds. Data is visualized as 4 charts representing signal interference marking the noise levels for each channel, signal interference spectrogram representing 60 samples for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

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

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

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

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



VLAN Probe

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

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

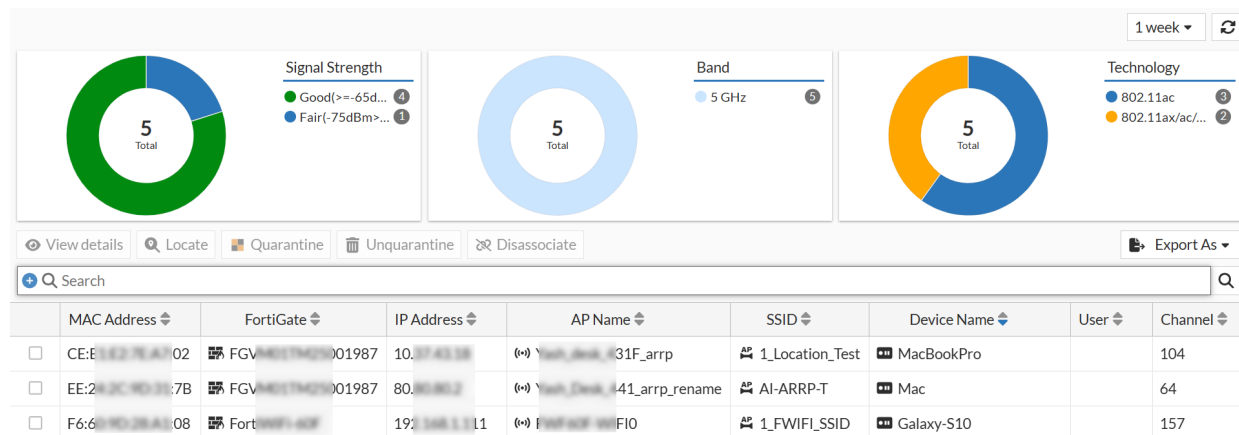
Select **Start** to initiate VLAN probe as per configurations.

Performance	Channel Summary	Clients	Interfering SSIDs	Logs	Spectrum Analysis	VLAN Probe
Probe Retries	10					
Timeout	5	Seconds				
VLAN Range	1	To	10			
<button>Start</button>						

Wireless Clients

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

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



Signal Strength

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

Band

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

Technology

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

The clients are listed with their relevant details, including the MAC address, FortiGate, IP address, FortiAP, SSID, channel, bandwidth, and signal strength.

View Details

To view detailed information about a client, select the desired client from the list and click **View Details**. See, [Clients Diagnostics and Tools](#).

Locate

Click the **Locate** to find the physical location of a wireless device. The system opens the **Wi-Fi Maps** window to highlight the placement of the selected wireless device on its floor plan. For more information, see [Locating Wireless Devices on the Map](#).

Quarantine

This button adds the device MAC address to a quarantine list, allowing FortiGate to apply security policies that block all or specific network access for that device.

- This button is available for both currently and previously connected clients.
- If a client is not quarantined, the button will show **Quarantine**. If it is already quarantined, the button will change to **Unquarantine**.
- Quarantined clients are also visually highlighted on the main **Wireless Clients** window (**Wireless > Wireless Clients**).

Unquarantine

This button enables you to remove a device MAC address from the quarantine list if previously added.

Disassociate

This button immediately disconnects a client from its access point.

Note: This option is only available when the time range is set to **Now**.

Export As

Click **Export As** to export the table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.

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

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

MAC Address	FortiGate	IP Address	Forti AP	SSID	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal St
00:09:58:35:00:04	FortiGate-300E	192.168.20.7	FW433C7F320000000	210_2Tunnel	161	2.49 kbps	7 dB	-88 dBm
00:09:58:35:00:02	FortiGate-300E	192.168.200.12	FW433C7F320000000	210_Bridge	132	0 bps	50 dB	-42 dBm
00:09:58:35:00:04	FortiGate-300E	192.168.20.7	FW433C7F320000000	210_Bridge	120	0 bps	56 dB	-43 dBm

Best Fit Columns

Reset Table

Select Columns

✓ MAC Address

✓ FortiGate

✓ IP Address

✓ Forti AP

✓ SSID

✓ Channel

✓ Bandwidth Tx/Rx

✓ Signal Strength/Noise

✓ Signal Strength

✓ Association Time

✓ FortiAP Radio

✓ VLAN ID

Authentication

Band

Bandwidth Rx

Bandwidth Tx

Device

Device OS

Encryption

FortiAP IP

Apply

Cancel

Wireless Clients Diagnostics and Tools

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

Diagnostics and Tools

SSID1_Location_Test

AP Name192.168.200.12_FortiGate-300E_431F_arp

Channel104(5GHz:802.11ac)

Quarantine

Disassociate

Locate

Status

Data Rates

Client Capabilities

AI Insights

Performance

Applications

Destinations

Policies

Logs

Good

SLA Health Score

1 week

Select All

Apply

Coverage

100%

AP Health

100%

Time To Connect

100%

Roaming

100%

Throughput

99.99%

Connection Failure

00.00%

05:35 PM

01:20 PM

09:06 AM

04:52 AM

12:38 AM

08:24 PM

04:10 PM

11:56 AM

07:42 AM

2025-12-06

07:30:00 AM - 09:29:59 AM

Connection Failure

Server Failure

192.168.200.12_FortiGate-300E_431F_arp

End

Close

The pane provides **Quarantine**, **Disassociate**, and **Locate** options. For more information, see [Wireless Clients](#).

On the right, the expand section consists of the following details:

- **Status:** This section provides a summary of Signal Strength, Band, Signal Strength/Noise, and Transmission Discard/Retry details.

- **Data Rates:** A summary of key data rate metrics, including Downlink and Uplink Data Rates, and their corresponding MCS (Modulation and Coding Scheme) Indexes.
- **Client Capabilities:** Displays client status for Optimized Roaming (802.11k), Fast Roaming (802.11r), and Assisted Roaming (802.11v). The capability is shown in green if it is supported and red if it is not supported. A **Client Connectivity** widget is also introduced providing an overview of the connection health of wireless clients. See [Wireless](#).

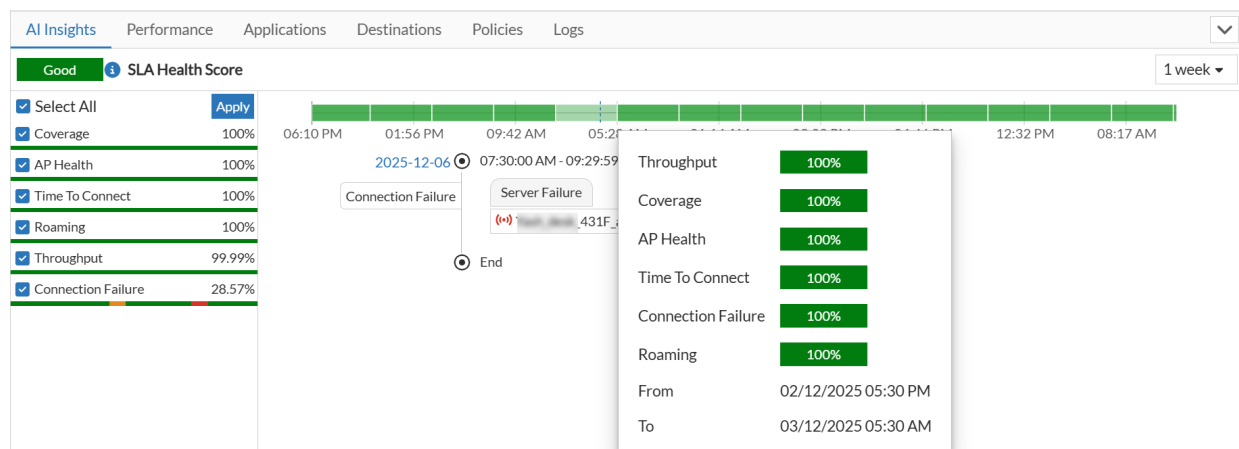
The **Diagnostics and Tools** pane has the following tabs to view more details:

- [AI Insights](#)
- [Performance](#)
- [Applications](#)
- [Destinations](#)
- [Policies](#)
- [Logs](#)

AI Insights

The **AI Insights** tab helps to analyze various performance metrics, identify issues, and provide detailed insights into the root cause of network problems, helping administrators maintain high service levels.

Note: This feature may not work as expected on Safari browser. For the best experience, use Chrome, Firefox, or Microsoft Edge instead.



The **SLA Health Score** provides the overall high-level score.

- **Good** for a score more 70
- **Fair** for a score between 30 and 70
- **Bad** for a score less than 30

Below the overall score, a list of individual SLAs or metrics is shown with their current health scores. You can select the SLAs that you want to track.

The following metrics are available:

- AP Health
- Roaming
- Coverage

- Throughput
- Connection Failure
- Time To Connect

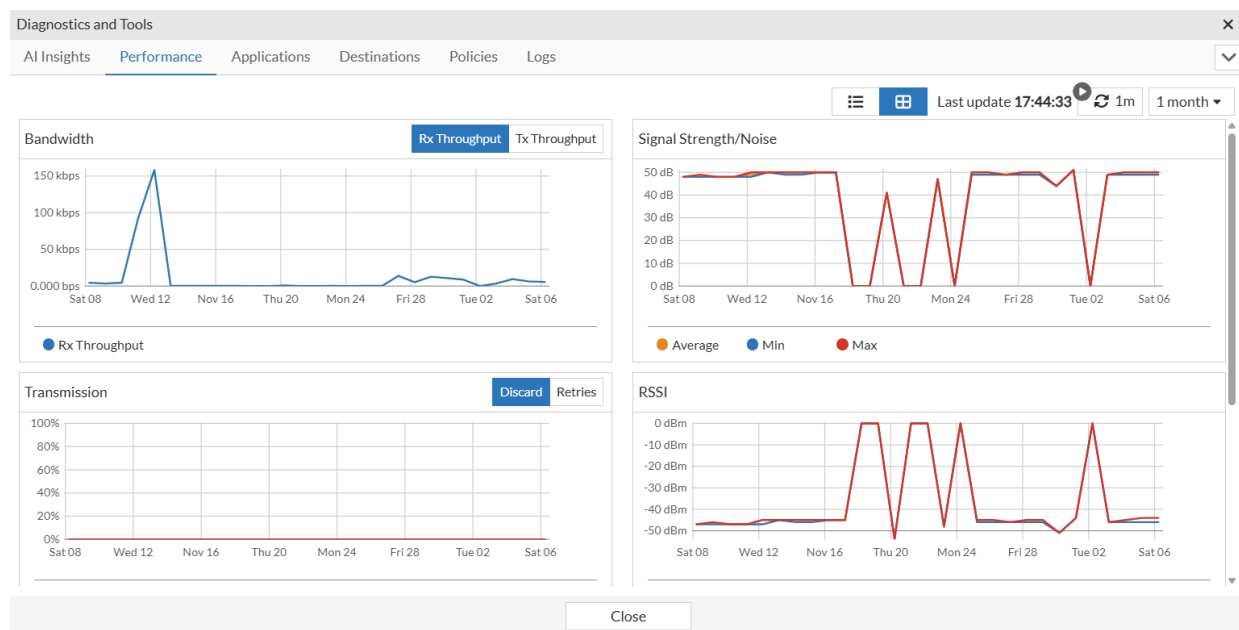
When you click an SLA, the corresponding **SLA Summary** window opens with more details.

The bar graph shows the performance trend over a selected time period (in this case, 1 day). The graph is divided to equal time segments. Based on the health score of each segment, the segments are colour coded as green (good), orange (fair), and red (bad).

Clicking on a specific time segment displays more details events that occurred during the time period.

Performance

The **Performance** tab displays information about the client's performance. You can filter the trends based on the selected duration or customized time slot; select a time window or define a **Custom range**. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**.



The following charts are available:

- **Bandwidth:** Displays the data transfer rate of the network over time, allowing you to monitor both Receive (Rx) and Transmit (Tx) throughput speeds.
- **Signal Strength/Noise:** Displays the Signal-to-Noise Ratio to assess connection quality. Higher values indicate a strong signal with minimal background interference.
- **Transmission:** Tracks the integrity and reliability of data packet delivery by monitoring specific metrics for discarded packets and retry attempts.
- **RSSI:** Displays the trend of Received Signal Strength Indicator (RSSI) over a selected time period for a client. RSSI is a measure of the Wi-Fi signal strength your device receives from an Access Point, typically measured in dBm (decibel milliwatts). A value closer to 0 dBm (for example, -30 dBm) indicates a strong signal, while a value closer to -90 dBm indicates a very poor one.

You can click on any point in the chart to see detailed information like **Timestamp, If Index, RSSI, Tx Data**

Rate, and Rx Data Rate.

- **Data Rate:** Shows the trend of data transmission speeds in both uplink (from the client to the access point) and downlink (from the access point to the client) directions for a client. You can view either of these trends at a time. The speeds are measured in Mbps (Megabits per second).

Similar to the RSSI chart, clicking on any point provides a detailed information like **Timestamp, If Index, Tx Data Rate, and Rx Data Rate.**

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.

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

Destinations

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

Now Search filterable columns					
☐	Destinations	Application	Bytes	Sessions	Bandwidth
☐	74.125.234.100	Google.Push.Notification	104.63 kB	2	0 B/s
☐	142.250.191.100	QUIC	71.79 kB	2	0 B/s
☐	157.140.1.100	Facebook	5.25 kB	2	0 B/s
☐	dns.google	SSL_TLSv1.3	16.87 kB	2	1.22 kB/s
☐	116.196.1.100	WhatsApp_File.Transfer	196.72 kB	1	409.83 kB/s
☐	172.217.14.100	Google.Services	14.86 kB	1	0 B/s

Policies

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

Now Search filterable columns						
☐	Policy	Policy Type	Source Interface	Destination Interface	Bytes	Bandwidth
☐	Tunnel_PSK-port1	policy	Tunnel_PSK	port1	1.27 MB	24 296 B/s

Logs

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

Search

Details

Date/Time	Level	Action	Message	SSID	Channel	Absolute C
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

Close

Channel Summary

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

- [Summary](#)
- [Events](#)
- [Insights](#)

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

Summary

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

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

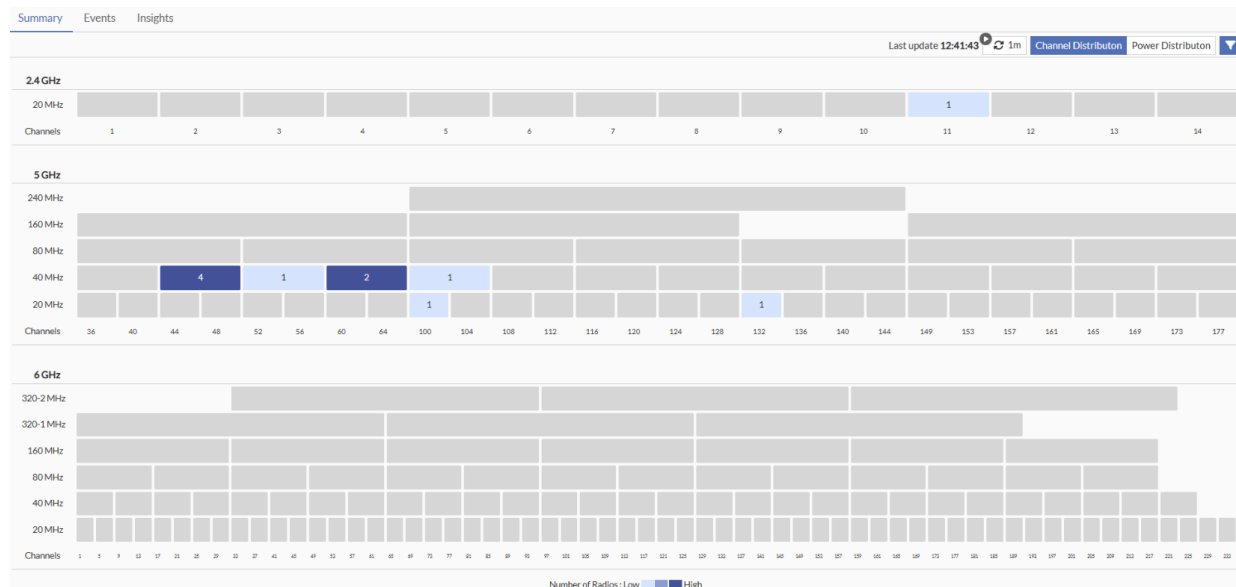
Channel Distribution

The **Channel Distribution** tab provides information about how the wireless network channels are utilized across different frequency bands. The information is categorized into three categories based on band namely – 2.4 GHz, 5 GHz, and 6GHz. Each band is further divided into different channel width - 20 MHz, 40 MHz, 80

MHz, 160 MHz, and so on. Hover over a channel number to view the number of radios operating on that channel.

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

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



Note:

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

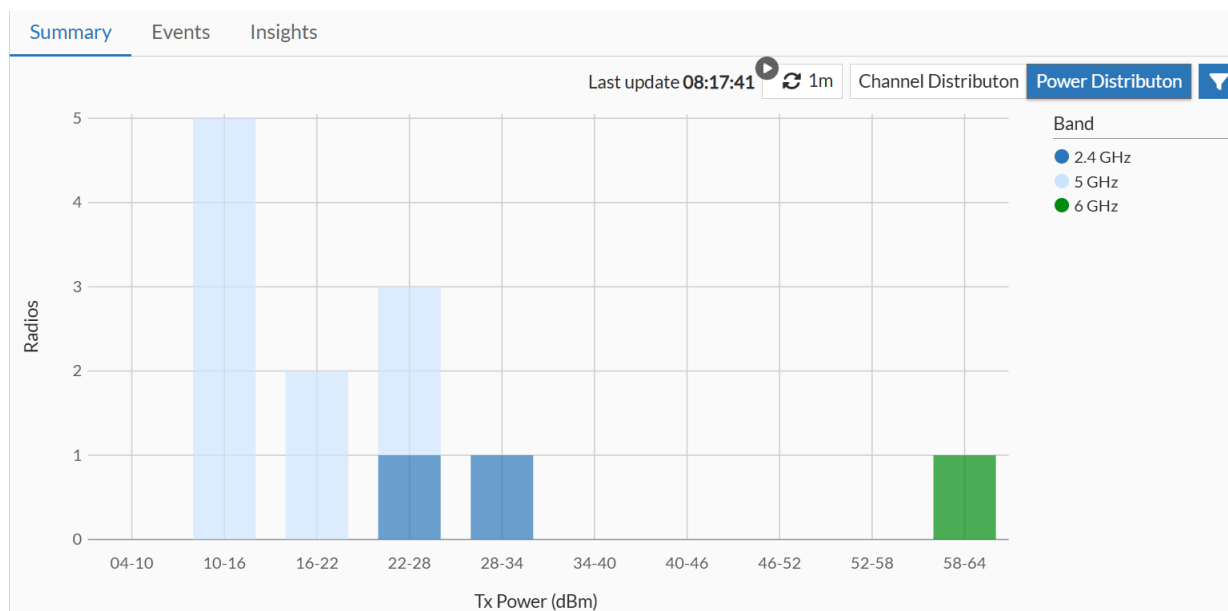
Power Distribution

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

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

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

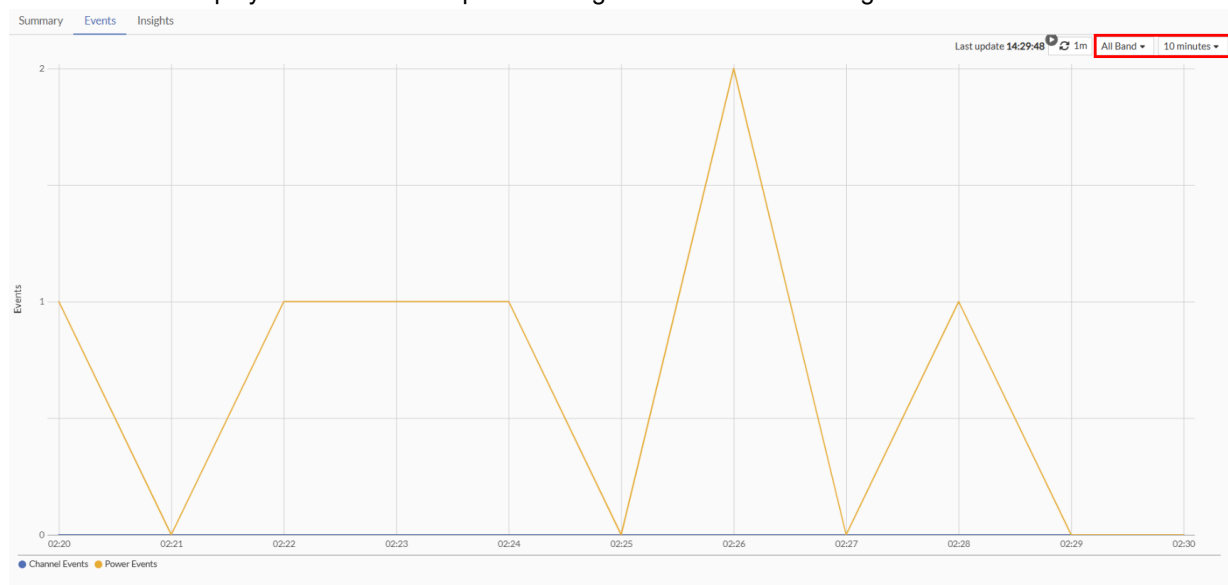
Use the **Filter** option to select FortiAPs and Radios at specific location such as Site, Building, and Floor.



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

Events

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



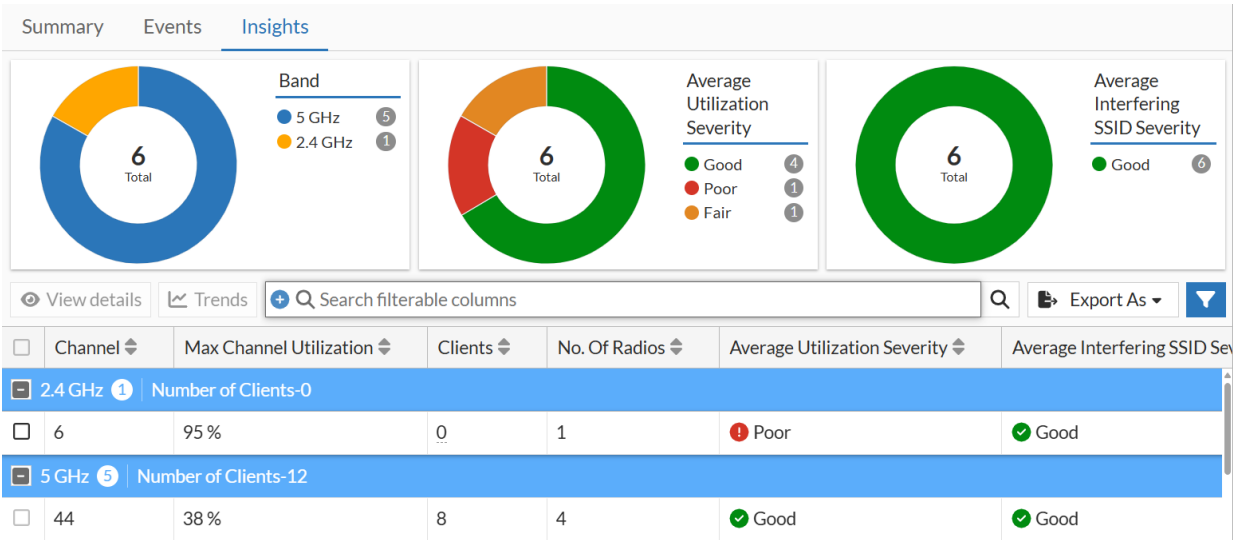
Select the desired bands and time period for the chart using the drop-down menus.

Insights

This page provides granular insights into the performance of each channel with key insights into critical statistics, that are key in determining the health of your wireless network. This facilitates effective resolution of

any potential network stability issues due to the operating channel. FortiAIOPS retrieves and aggregates all channel related statistics from the FortiAPs operating in your network and multiple radios operating on various channels.

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



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

Floor Section

Site:

Building:

Floor:

The following charts are available:

- [Band](#)
- [Average Utilization Severity](#)
- [Average Interfering SSID Severity](#)

Band

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

Average Utilization Severity

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

Average Interfering SSID Severity

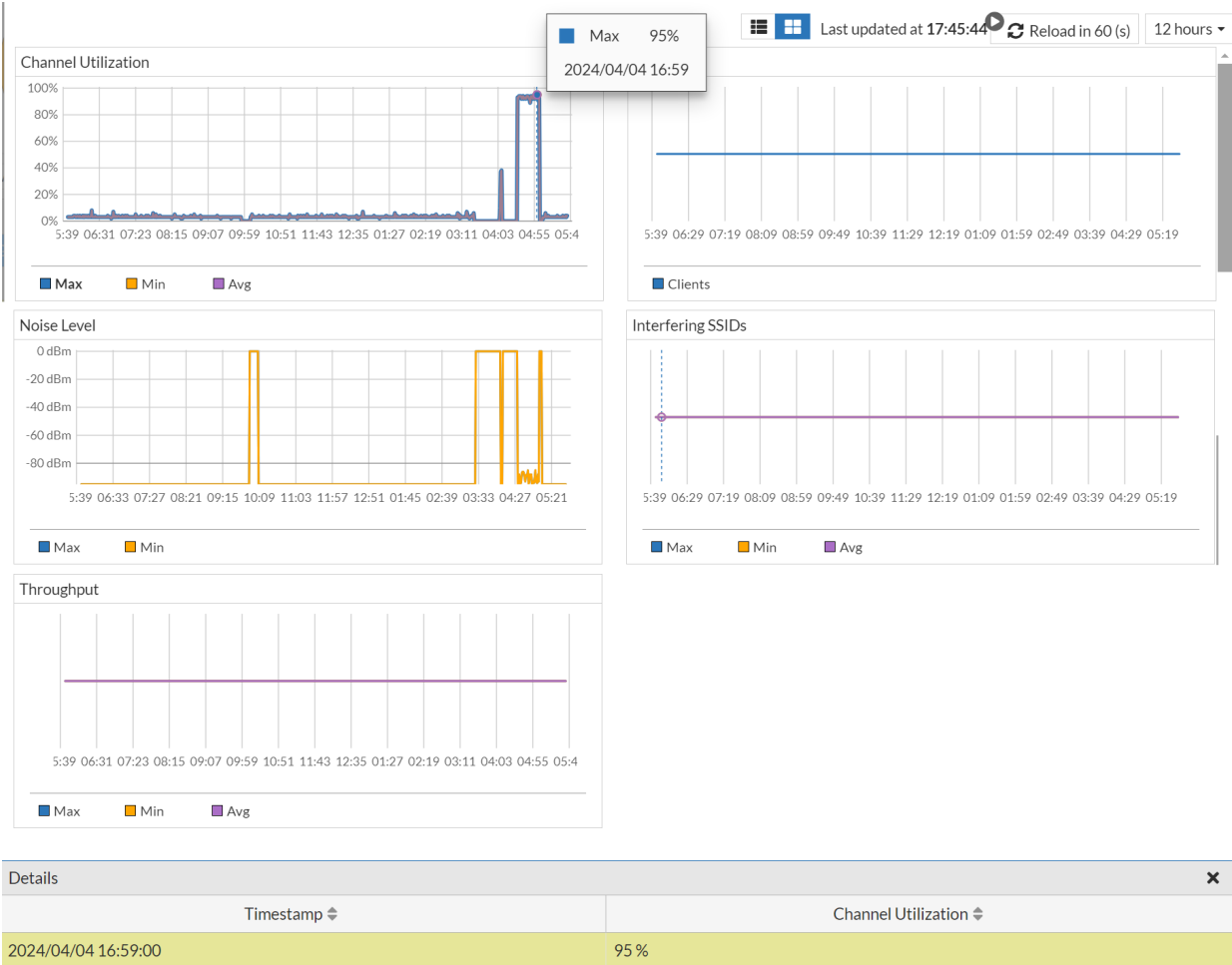
This chart provides the channel count based on the average interfering SSID severity over the last 60 seconds. FortiAIOPS automatically categorizes the channels as **Good** or **Poor**, and **Fair**. The total number of channels for each severity are displayed along with what percentage of the total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

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

Channel-6(2.4 GHz) ×							
+ Q Search filterable columns Q							
FortiGate Name	AP Name	Radio	Channel Utilization	Clients	Throughput	Utilization Severity	Interfering SSID Severity
FGT_PRIMARY	HA_3flab	1	3%	0	0 B/s	Good	Good

Field	Description
FortiGate Name and AP Name	The names of the FortiGate controller and FortiAP associated with the selected channel.
Radio	The radio operating on the selected channel.
Channel Utilization	Total channel utilization (in percentage) per radio.
Clients	The number of clients connected per radio.
Throughput	The total throughput of traffic passing per radio.
Utilization Severity	The average utilization severity of the selected channel.
Interfering SSID Severity	The average interfering SSID severity of the selected channel.
SSIDs	The SSIDs associated with the radio.
Noise Level	The noise level detected by the by the radio.
Health Assessment	FortiAIOPS evaluates a assigns the health status of each radio.

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



Click **Export As** to export the table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.

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

AI-ARRP

AI-ARRP is an advanced, AI-driven system that automates and optimizes the management and distribution of wireless channels across all Access Points (APs) monitored by FortiAI Ops. The AI engine makes precise channel decisions by leveraging historical telemetry and deep insights gathered by FortiAI Ops.

The accuracy of AI-ARRP stems from its ability to optimally score every available channel for each FortiAP radio. This scoring uses critical RF metrics, including noise levels, channel utilization, interfering APs, rogue APs, and spectral RSSI. FortiAI Ops achieves this accuracy by analyzing real-time RF conditions along with up to two weeks of historical channel data to generate reliable channel scores and recommend a better channel for the AP radio.

To use the FortiAI Ops AI-ARRP engine, you must enable both `ai-darrp-support` and `darrp` within the FortiAP (WTP) profile (see [DARRP with FortiAI Ops managed FortiGates](#)).

Use the following commands:

```
config wireless-controller wtp-profile
  edit <name>
    config radio-1
      set ai-darrp-support enable
      set darrp enable
    next
  next
end
```

Note: By default, `ai-darrp-support` is disabled.

The combination of the `darrp` and `ai-darrp-support` commands determine how FortiGate and FortiAIOps handle channel selection and data collection.

darrp	ai-darrp-support	Description
disable	enable	Local DARRP is inactive. FortiAIOps collects telemetry data using GET REST-APIs but cannot make changes.
enable	enable	The FortiAIOps engine takes control. It collects data and actively triggers channel changes using POST REST-APIs.

Note:

- You must add FortiGate to FortiAIOps with administrative privileges for accurate collection of data.
- It is recommended to enable both `darrp` and `ai-darrp-support` to leverage the FortiAIOps AI-ARRP capabilities.
- You can enable AI-ARRP from FortiAIOps GUI for Non AI-ARRP radios. See [Detailed Analysis and Optimization](#).

Once enabled, the FortiAIOps AI-ARRP engine performs the following actions:

1. **Data Collection:** RF statistics for all channels on each AP radio are collected every minute.
2. **Analysis and Daily Channel Health Forecast:** The collected data is aggregated every hour, and the system evaluates the health of each available channel for that AP radio. The AI-ARRP model evaluates current channel health metrics along with up to two weeks of historical RF data, and generates daily forecast of channel performance for each radio.
3. **DARRP Schedule and Channel Validations:** During the scheduled DARRP window on the FortiGate, AI-ARRP analyzes and performs a series of critical validation checks, including:
 - Channel availability based on the FortiAP profile
 - Mandatory regulatory compliance (country code and indoor/outdoor channel rules)
 - Non-overlapping channel requirements and channel bonding considerations
 - Channel failures related to Wireless SLAs and any radar detections
4. **Final Channel Push:** The finalized recommended channels for each radio are securely pushed to the FortiGate, and the FortiAPs use these updated channel assignments in their next channel planning cycle.

Note: AI-ARRP is only supported on FortiOS 7.6.5 and FortiAP version 7.6.3.

The **AI ARR**P window is available under the **Wireless** menu.



Filtering

The **AI ARRPP** window consists of four primary widgets and offers the following filtering capabilities:

Filters

Use the filters at the top to select **Floor**, **FortiGate**, and **Bands**.

- **Floor:** Select **Floor** filter and in the **Floor Selection** pane, choose the required **Site**, **Building** and **Floor** using the drop down.
- **FortiGate:** Select the **FortiGate** filter and from the **Dashboard Filters** pane select the required **FortiGate**.
- **Bands:** Select the necessary bands from the **Bands** filter.

Timeline

Select the monitoring timeline from the drop down. Choose between **4 hours**, **6 hours**, **1 day**, and **1 week**.

- [Monitoring Widgets](#)
- [Detailed Analysis and Optimization](#)
- [Disabling AI-ARRP](#)

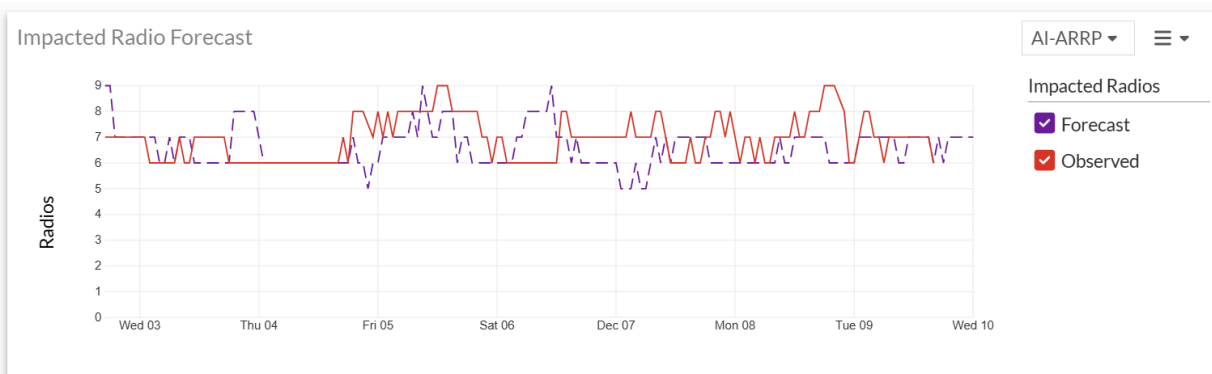
Monitoring Widgets

The **AI ARRPP** window consists of four primary widgets designed to analyze the impact and reasons behind channel changes and radio health.

Note: To add the required widget to the dashboard, click **Add Widget** and from the **Wireless > AI ARRPP** section, select a widget and click **+**.

Impacted Radio Forecast

This chart visualizes the difference between the observed (actual) and the forecast count of problematic radios by plotting the number of impacted radios against a specific time period.



The chart displays two key metrics:

- **Observed:** This line represents the real-time count of impacted radios that the system currently identifies as unhealthy or impacted.
- **Forecast:** This line shows the predicted count of impacted radios that the AI-ARRP model estimates will be impacted.

You can filter the displayed radio data using the drop-down menu to view specific management types:

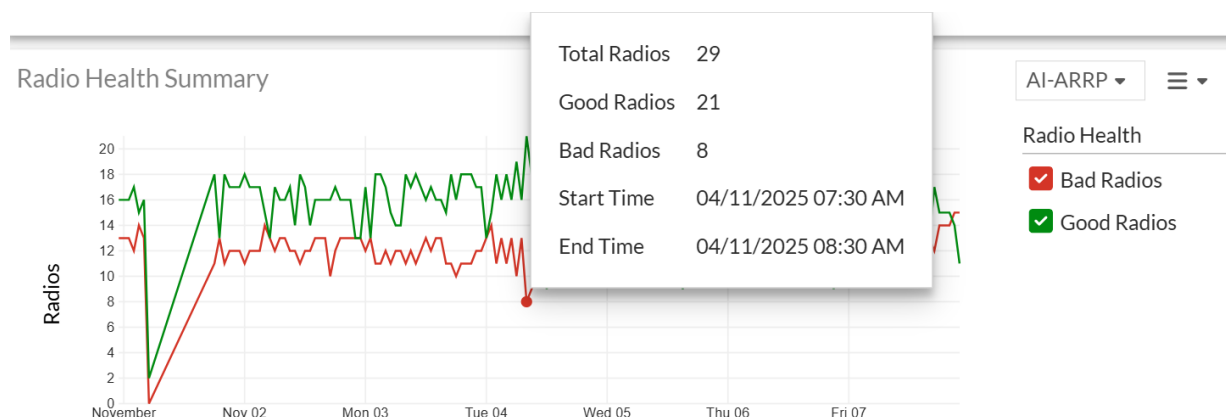
- **AI-ARRP:** Displays details only for radios where the AI-ARRP feature is enabled.
- **Non-AI-ARRP:** Includes radios where traditional DARRP is either enabled or disabled.
- **All:** Shows data covering both AI-ARRP managed radios and Non-AI-ARRP radios.

Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the details pane. See [Detailed Analysis and Optimization](#).

Radio Health Summary

The **Radio Health Summary** chart shows the overall status of all AP radios by comparing how many radios are operating on good channels versus bad channels over time. Radios on good-performing channels are counted as **Good Radios**, while those running on poor-performing channels are counted as **Bad Radios**.



You can filter the displayed radio data using the drop-down menu to view specific management types:

- **AI-ARRP**: Displays details only for radios where the AI-ARRP feature is enabled.
- **Non-AI-ARRP**: Includes radios where traditional DARRP is either enabled or disabled.

Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the details pane. See [Detailed Analysis and Optimization](#).

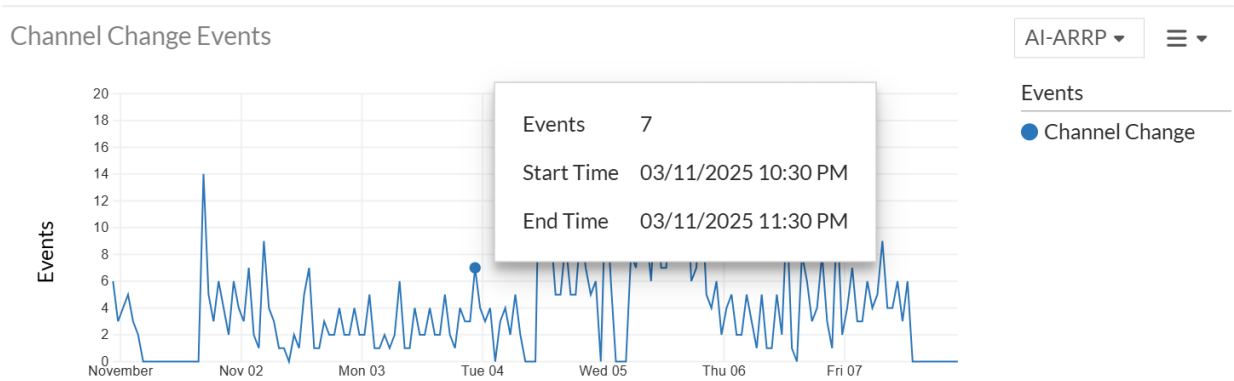
Channel Change Events

This chart provides detailed visibility into all channel change events triggered by the radio provisioning system. It captures channel changes initiated through both AI-ARRP from FortiAIOPs and DARRP from Fortigate.

When the **AI-ARRP** filter is applied, the chart shows all channel changes recommended by AI-ARRP.

When the **Non-AI-ARRP** filter is applied, it displays channel changes triggered by DARRP.

The chart shows how many times AP radios across the network switched their operating channel within the selected time period.



Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the **Details** pane.

Details							
Search filterable columns						Details	
	Date/Time	Level	Action	Message	SSID	AP Name	
Events	2025/11/04 06:48:07	■■■■■■■■	ai-darrp-channel	AP [redacted]_441_arrp radio 3 channel ...	N/A	[redacted]_441_ar	
	2025/11/04 06:48:07	■■■■■■■■	ai-darrp-channel	AP [redacted]_231G-arrp radio 2 channel ...	N/A	[redacted]_231G-ar	
	2025/11/04 06:46:37	■■■■■■■■	ai-darrp-channel	AP [redacted]_231G-arrp radio 1 channel ...	N/A	[redacted]_231G-ar	
	2025/11/04 06:46:37	■■■■■■■■	ai-darrp-channel	AP [redacted]_441_arrp radio 2 channel ...	N/A	[redacted]_441-ar	
	2025/11/04 06:46:37	■■■■■■■■	ai-darrp-channel	AP [redacted]_243K_arrp radio 1 channe...	N/A	[redacted]_243K-i	
5 Updated: 23:06:25						Close	

The table in the **Details** pane provide details such as **Date/Time**, **Level**, **Action**, **Message**, **SSID**, **AP Name**, **Log ID**, **FortiGate Serial Number**, and **Channel**.

Select an event and click  icon to view further details.

+

Add

Details

×

🔍

Search filterable columns

Details

	Date/Time	Level	Action	Message	SSID
☒	2025/11/04 06:48:07		ai-darrp-channel	AP [redacted] 11_arrp.radio 3...	N/A
☐	2025/11/04 06:48:07		ai-darrp-channel	AP [redacted] LG_arrp.radio 2...	N/A
☐	2025/11/04 06:46:37		ai-darrp-channel	AP [redacted] LG_arrp.radio 1...	N/A
☐	2025/11/04 06:46:37		ai-darrp-channel	AP [redacted] 11_arrp.radio 2...	N/A
☐	2025/11/04 06:46:37		ai-darrp-channel	AP [redacted] 3K_arrp.radio ...	N/A

5 Updated: 23:06:25

↻

Close

General

Absolute Date/Time 2025/11/04 06:48:07

Time 06:48:08

Virtual Domain root

Log Description Physical AP radio DARRP channel change from AI

Source

MAC Address N/A

Interface 3

SSID N/A

User N/A

Action

Action ai-darrp-channel

Reason N/A

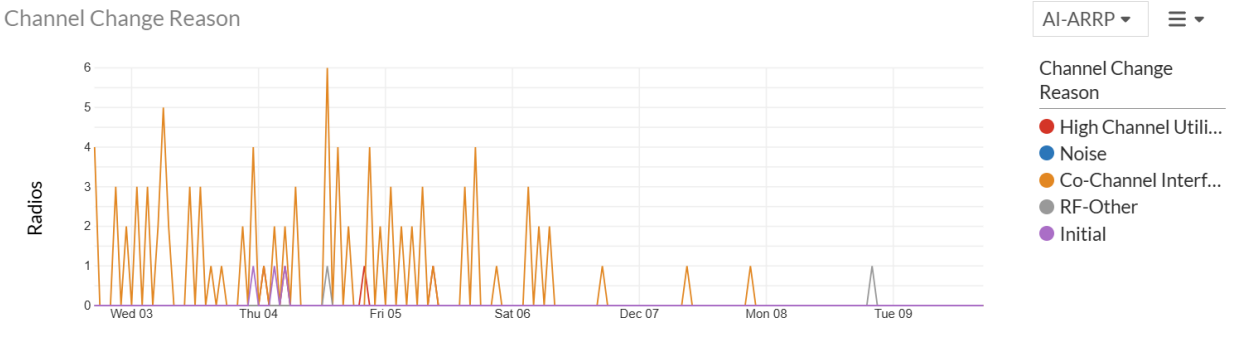
Security

Close

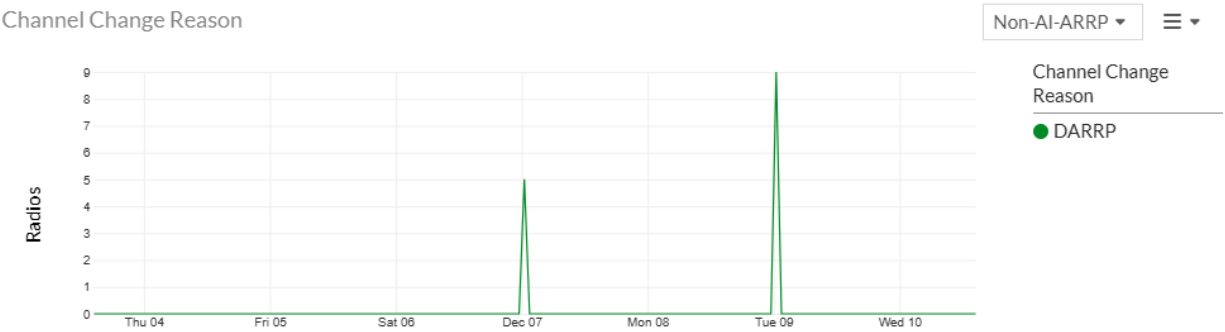
Channel Change Reason

This widget provides a detailed breakdown of the factors that prompted AI-ARRP to recommend a channel change, highlighting the key conditions that affected the health of the current operating channel. The reasons reported include:

- High Channel Utilization
- Noise
- Co-channel Interference (neighboring APs detected on overlapping channels)
- RF-Other (such as Spectral RSSI)
- Initial (channel change applied based on FortiGate results)



When the **Non-AI-ARRP** filter is applied, the widget displays the reason as DARRP, indicating that the channel change was recommended by FortiOS DARRP.



Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the details pane. See [Detailed Analysis and Optimization](#).

Detailed Analysis and Optimization

Clicking on a data point in the **Impacted Radio Forecast** or **Radio Health Summary** or **Channel Change Reason** charts opens a pane for detailed analysis and action.

Observed Impacted Radio Details

View details Optimize Search

	Date/Time	AP Name	AP Profile	DARRP Profile	Band	Operating Channel	Radio Health
☐	2025/11/16 12:00:05	rad desk-441-arrp	FAP-radar	arrp-radar	2.4GHz	1	Bad
☐	2025/11/16 12:00:04	rad desk-441-arrp	Urad-441k-Schedule	arrp-schedule	2.4GHz	11	Bad
☐	2025/11/16 12:00:04	rad desk_431F_arrp	FAP431F-default	arrp-onetime	2.4GHz	1	Bad
☐	2025/11/16 12:00:04	rad desk_243K_arrp	FAP243K-Neighbor	arrp-neighbour	2.4GHz	6	Bad
☐	2025/11/16 12:00:03	rad desk-231G-arrp	FAP231G-default	arrp-neighbour	2.4GHz	11	Bad
☐	2025/11/16 12:00:03	rad desk_441_arrp	Yad desk-441K-neighbor	arrp-neighbour	2.4GHz	1	Bad
☐	2025/11/16 12:00:02	rad desk_441_arrp	Shad desk-441k	arrp-default	2.4GHz	1	Bad

7 Updated: 20:56:42

Close

The table displays information such as **Date/Time**, **AP Name**, **AP Profile**, **DARRP Profile**, **Band**, **Operating Channel**, **Radio Health**, **Radio Health Summary**, **Radio ID**, **Channel Change Reason**, **FortiGate Name**, **AP Serial Number**, **FortiGate Serial Number**, and **Last Channel Change**.

Optimize

Select an AP radio and click **Optimize** to manually trigger an immediate channel planning on that radio. This action evaluates the current RF environment and recommends the most optimal operating channel. Unlike the scheduled AI-ARRP runs, this channel-planning operation occurs instantly and may impact connected clients if performed during business hours.

Note: Optimize can be performed only on radios impacted in last 1 hour.

Observed Impacted Radio Details							
Optimizes radio performance by automatically assigning the best available channel using AI-ARRP.							
View details Optimize Search filterable columns							
	Date/Time	AP Name	Forti AP Profile	DARRP Profile	DARRP	AI-ARRP	Band
☐	2025/12/09 16:30:06	(📶) ATO-441K-2	FAP-441K-test	test	✓ Enabled	✓ Enabled	5GHz
☒	2025/12/09 16:30:06	(📶) ATO-441K-1	FAP-441K-test	test	✓ Enabled	✓ Enabled	5GHz
☐	2025/12/09 16:30:06	(📶) ATO-441K-1	FAP-441K-test	test	✓ Enabled	✓ Enabled	2.4GHz
☐	2025/12/09 16:30:05	(📶) ATO-441K-2	FAP-441K-test	test	✓ Enabled	✓ Enabled	2.4GHz
☐	2025/12/09 16:30:05	(📶) ATO-441K	FAP241K-AI-ARRP	test	✓ Enabled	✓ Enabled	2.4GHz
☐	2025/12/09 16:30:05	(📶) ATO-441K	FAP241K-AI-ARRP	test	✓ Enabled	✓ Enabled	5GHz

Enable AI-ARRP

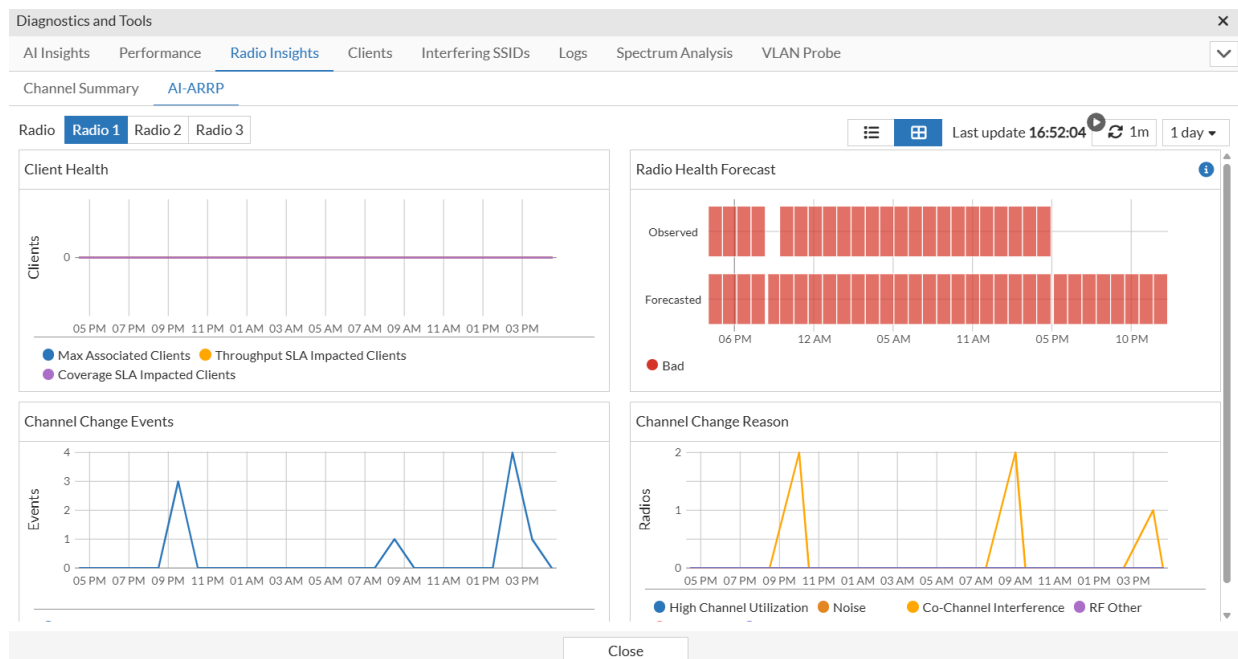
You can enable AI-ARRP from FortiAI Ops for Non AI-ARRP radios. To enable, select the Non AI-ARRP radios impacted in the last 1 hour and click **Enable AI-ARRP**.

Radio Details							
Enables AI-driven ARRP support on the selected radio.							
View details Enable AI-ARRP Search filterable columns							
	Date/Time	AP Name	Forti AP Profile	DARRP Profile	DARRP	AI-ARRP	Band
☒	2025/12/09 16:30:07	(📶) ATO-441K	FAP-441K-AI-ARRP	N/A	✗ Disabled	✗ Disabled	6GHz
☐	2025/12/09 16:30:06	(📶) CH-441K-01	FAP-441K-default	N/A	✗ Disabled	✗ Disabled	2.4GHz
☐	2025/12/09 16:30:06	(📶) CH-441K-02	FAP-441K-default	N/A	✗ Disabled	✗ Disabled	2.4GHz
☐	2025/12/09 16:30:06	(📶) BR-241K-BACK	FAP-241K	arrp-default	✓ Enabled	✗ Disabled	2.4GHz
☐	2025/12/09 16:30:06	(📶) BR-441K-Living	FAP-441K	arrp-default	✓ Enabled	✗ Disabled	6GHz

View Details

Select an AP and click **View Details** to open the dedicated **Details** pane for the selected radio.

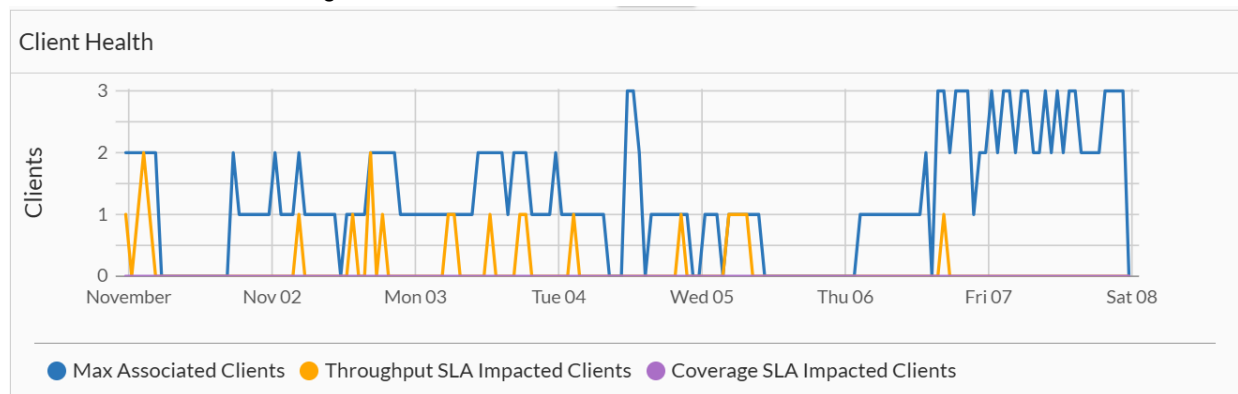
Note: Similar insights are available for individual Access Points on a per-radio basis by navigating to **Wireless > Access Points**. Select the desired AP, click **View Details**, and then go to the **Radio Insights** tab and the **AI-ARRP** sub-tab.



The following charts are displayed:

Client Health

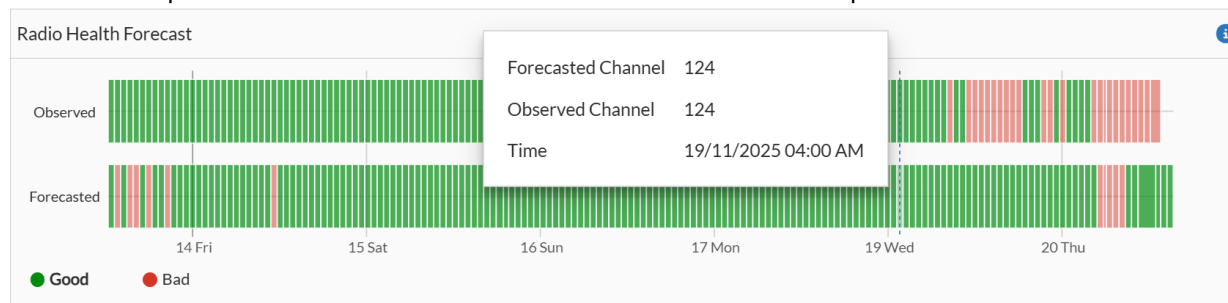
This chart tracks the following client-related issues over time.



- **Max Associated Clients:** Shows the maximum number of clients associated with this specific radio.
- **Throughput SLA Impacted Clients:** Tracks clients whose throughput is falling below the configured Service Level Agreement (SLA).
- **Coverage SLA Impacted Clients:** Tracks clients experiencing poor coverage.

Radio Health Forecast

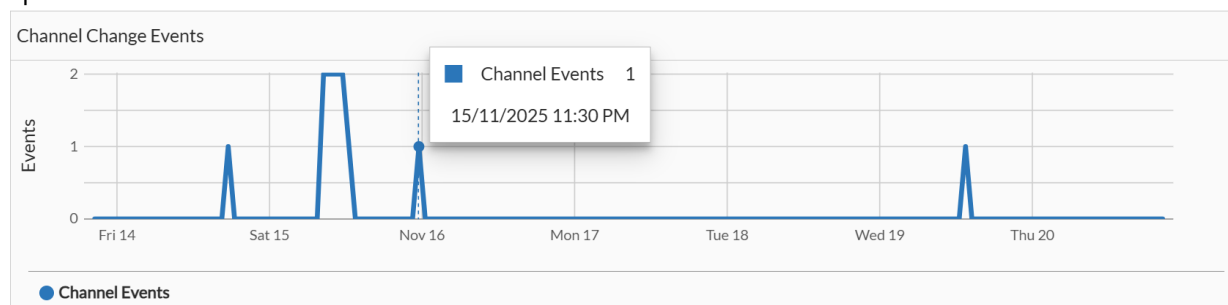
This bar chart provides a visualization of the radio health over the monitored period.



- **Observed:** Shows the actual periods when the radio's health was good or bad on operating channel. Red bars indicate periods when the radio's channel health was bad, while green bars represent periods when the radio was operating with good channel
- **Forecast:** Shows the periods when the AI-ARRP model predicted that the radio health on channel would be impacted. This helps evaluate the accuracy of the AI prediction against the observed reality.

Channel Change Events

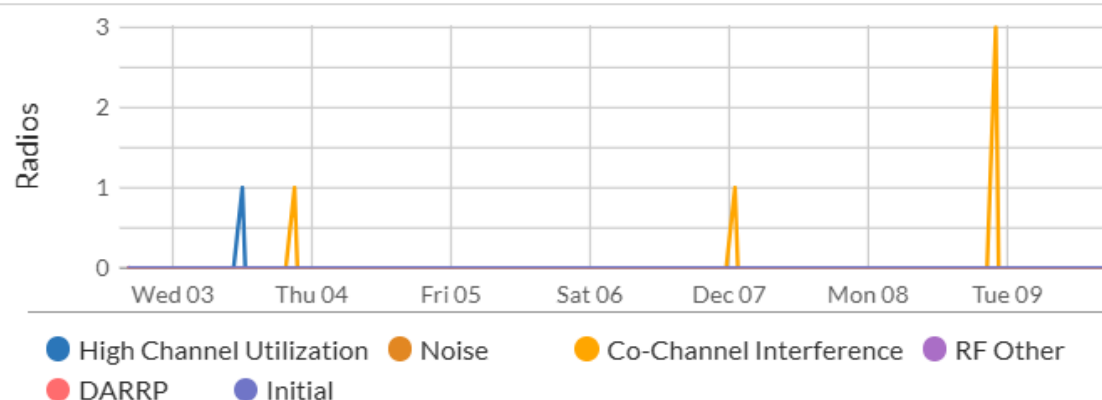
This chart displays a time-series graph showing the number of channel change events that occurred for this specific radio.



Channel Change Reason

This chart categorizes why the channel change events took place. It identifies the specific trigger for the channel switches such as **High Channel Utilization**, **Noise**, **Co-Channel Interference**, **RF Other**, or **DARRP**.

Channel Change Reason



Disabling AI-ARRP

You can disable AI-DARRP support on a per-radio basis using the FortiAP CLI WTP profile. Use the `set ai-darrp-support` command to enable or disable AI-ARRP on any radio.

```
#config wireless-controller wtp-profile
#edit FAP243K-default
# config radio-1
# set ai-darrp-support
enable Enable support for FortiAIOPS REST API calls for DARRP data.
disable Disable support for FortiAIOPS REST API calls for DARRP data.
```

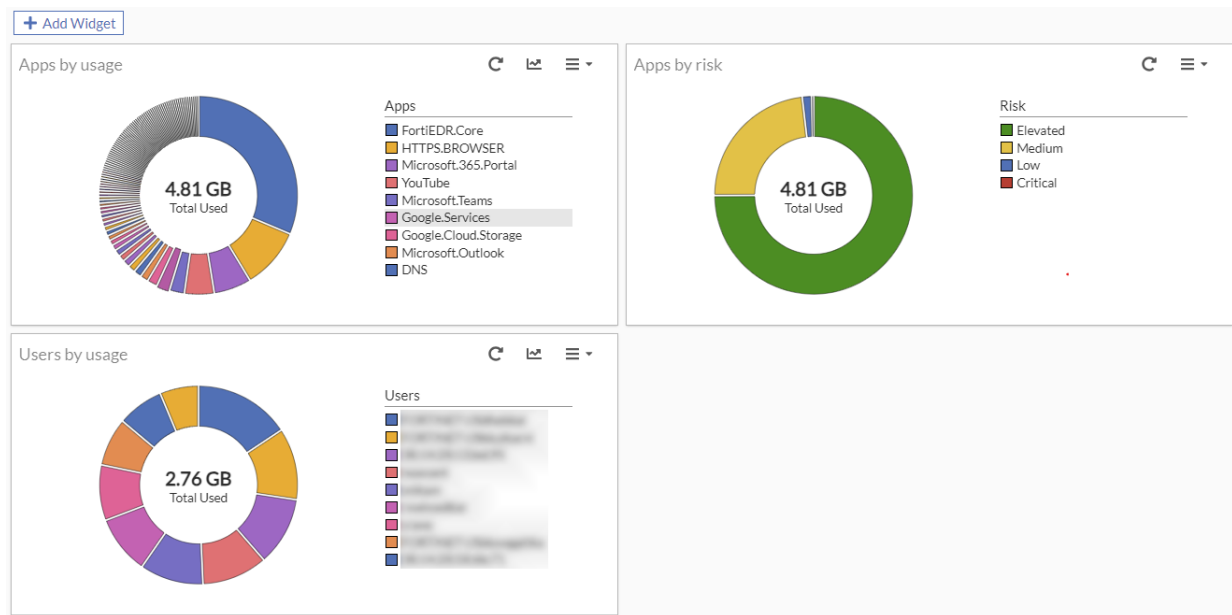
```
FGVM01TM25001987 (radio-1) # set ai-darrp-support
enable Enable support for FortiAIOPS REST API calls for DARRP data.
disable Disable support for FortiAIOPS REST API calls for DARRP data.
```

Note: For AI-DARRP to function correctly, both `darrp` and `ai-darrp-support` must be enabled in the WTP profile.

```
ai-darrp-support : enable
darrp : enable
arrp-profile : arrp-default
max-clients : 0
```

Applications

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

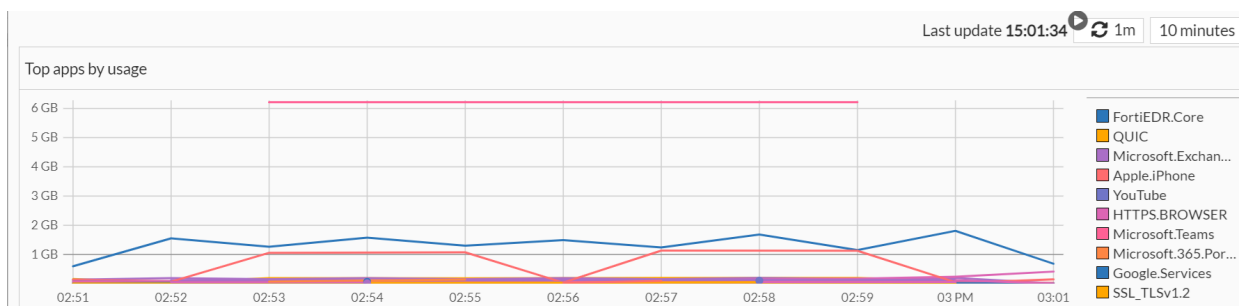


Apps by usage

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

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

Click on the trends icon  to view the application usage trends. You can filter the trends based on the selected duration or customized time slot; select a time window or define a **Custom range**. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**.



Apps by risk

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

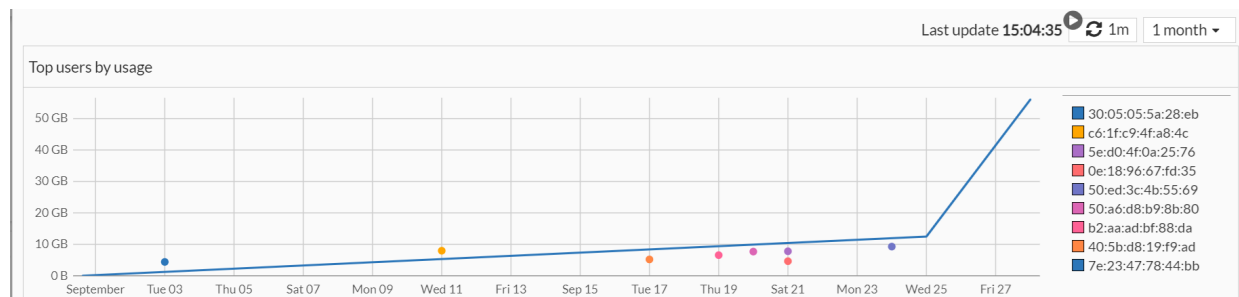
Top Applications By Risk				
Search filterable columns				
☐	Application	Usage	Risk Level	Users
☐	HTTPS.BROWSER	524.02 MB	Medium	56
☐	Facebook	81.95 MB	Medium	9
☐	Microsoft.Outlook	76.69 MB	Medium	11
☐	Microsoft.Exchange.Server	62.39 MB	Medium	42

User by usage

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

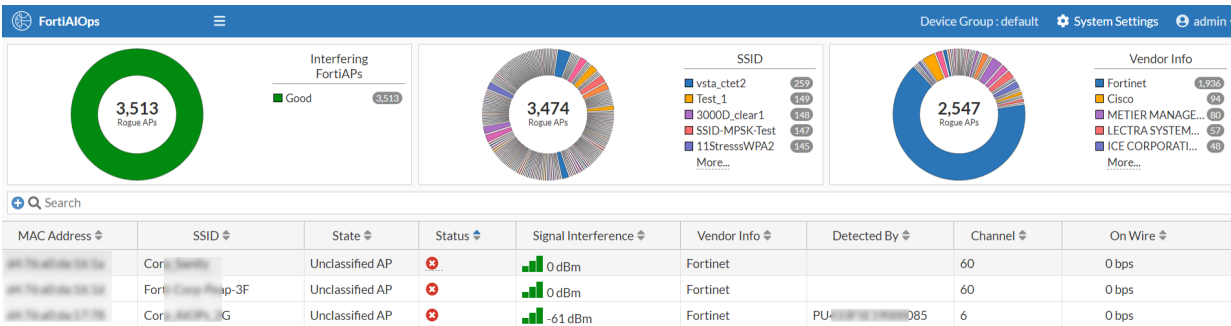
Top Users By Usage					
Search filterable columns					
☐	User	Applications	Access Points	SSID	Usage
☐		16	1	1	637.68 MB
☐		20	1	1	414.89 MB
☐		21	1	1	398.02 MB
☐		21	2	1	328.01 MB

Click on the trends icon  to view the application user trends. You can filter the trends based on the selected duration or customized time slot; select a time window or define a **Custom range**. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**.



Rogue APs

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



Interfering APs

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

SSID

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

Vendor Info

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

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

Click **Export As** to export the table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.

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

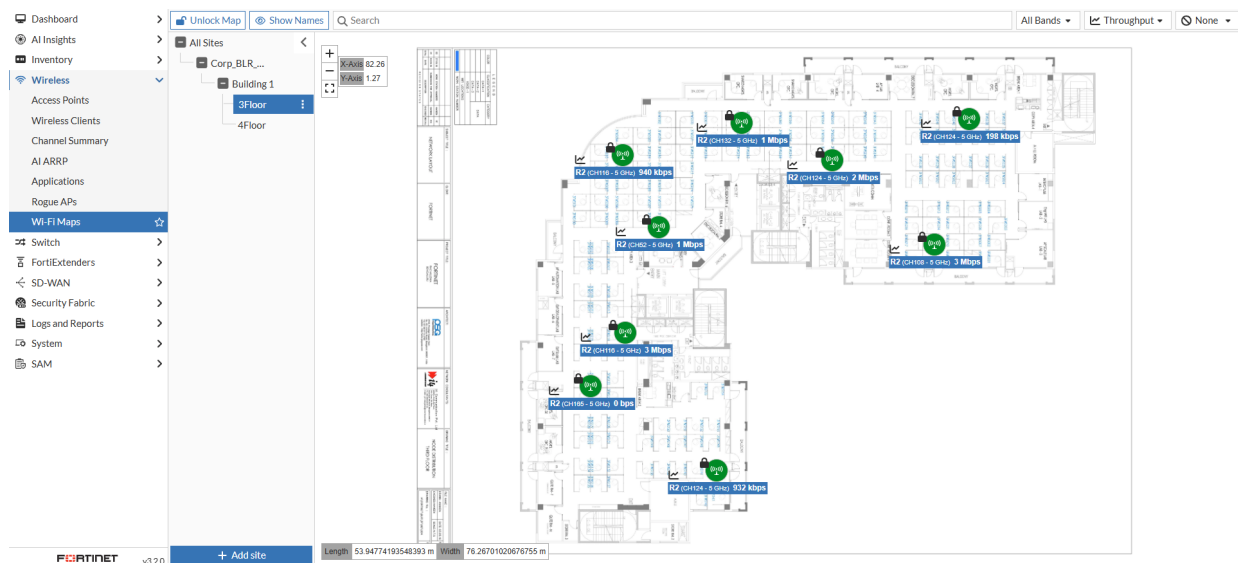
Wi-Fi Maps

Wi-Fi Maps provides a powerful visual representation of the physical layout of your site, letting you to accurately map your access points (APs). It features seamless compatibility with **Eka**hau, a leading Wi-Fi planning tool. You can easily modify maps by importing and exporting .esx files to add sites, buildings, floors, and AP locations, and then export the updated map back to Eka

Wi-Fi Maps offers real-time status and alerts for your FortiAPs, providing quick visualization of each unit on custom floor plans. This is enhanced by a **Locate** feature available across all wireless management screens, enabling you to instantly pinpoint the physical location of any Access Point or wireless client directly on the maps.



- After upgrading to Release 3.2.0:
- All valid floor maps will be successfully migrated to the new **Wi-Fi Maps** feature.
 - All existing FortiAP placements and their configured features will be fully retained and carried over to the new system.

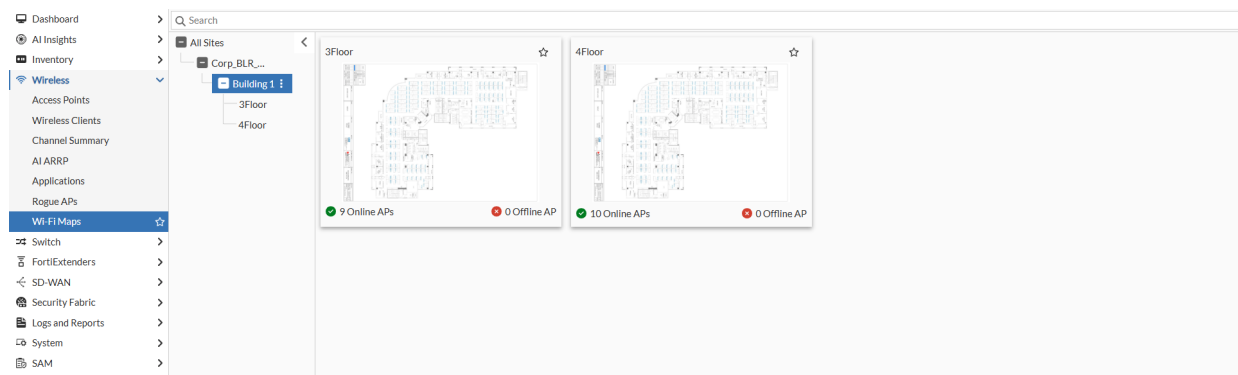


- [Creating the Map Structure](#)
- [Importing and Exporting Maps](#)
- [Modifying the Map](#)
- [Viewing the Map](#)
- [Diagnostics and Tools](#)
- [Locating Wireless Devices on the Map](#)

Creating the Map Structure

The map structure is organized hierarchically, starting with the largest entity: **Site** > **Building** > **Floor**.

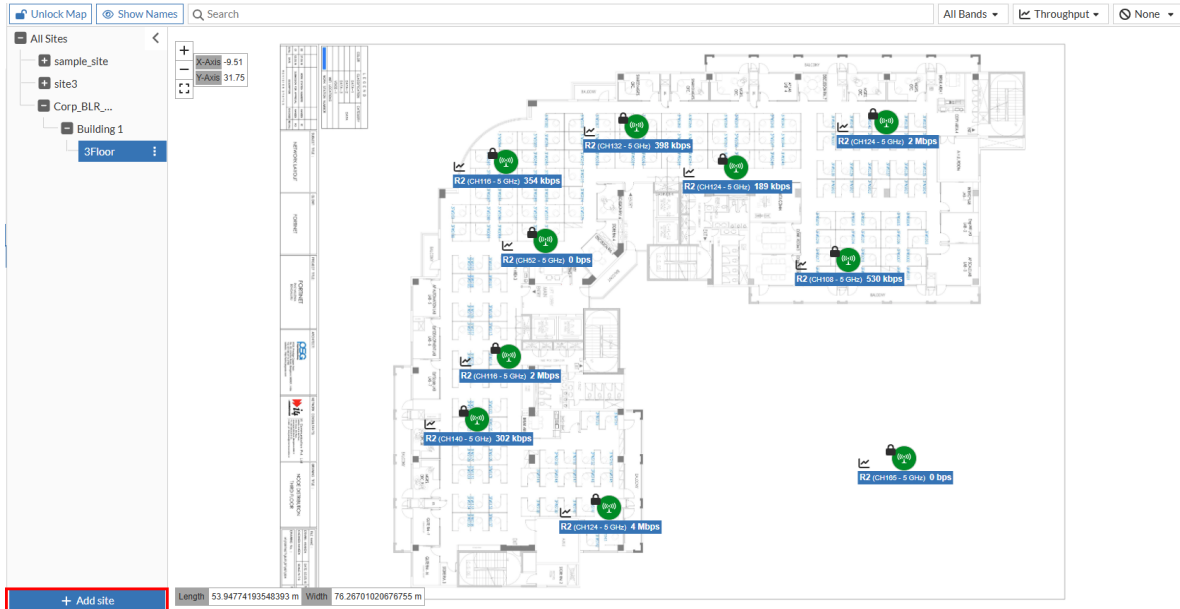
- [Adding a Site](#)
- [Adding a Building](#)
- [Adding a Floor](#)



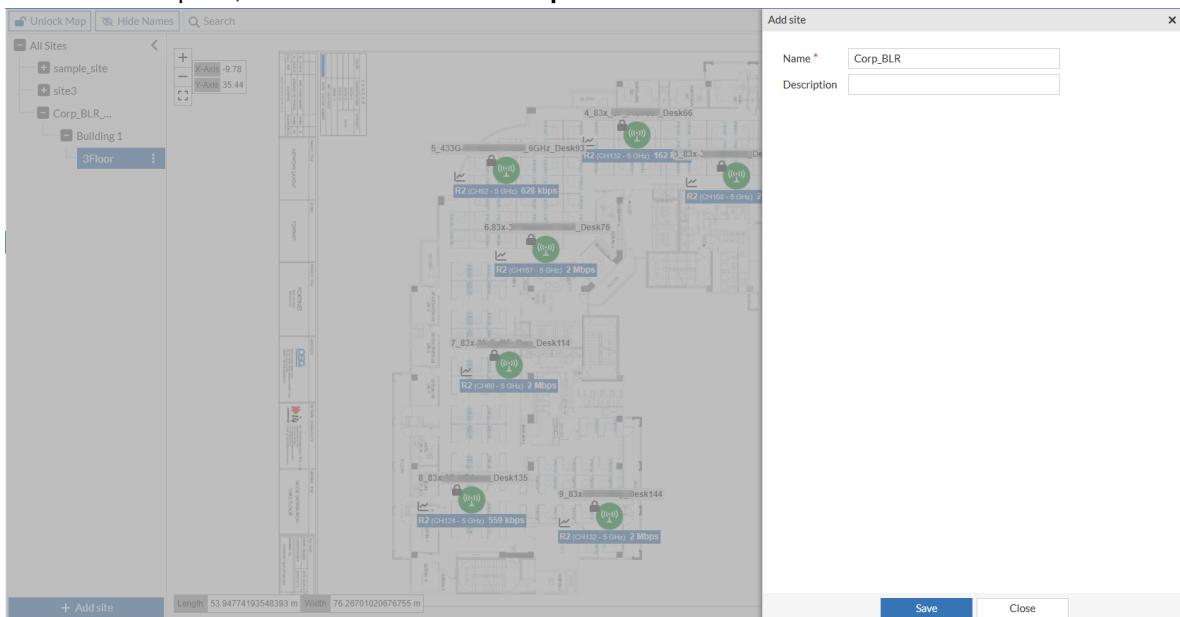
Adding a Site

A site is the top-level entity that contains multiple buildings.

1. Navigate to **Wireless > Wi-Fi Maps**.
2. Click **Add site**.



3. In the **Add site** pane, enter a **Name** and a **Description**.



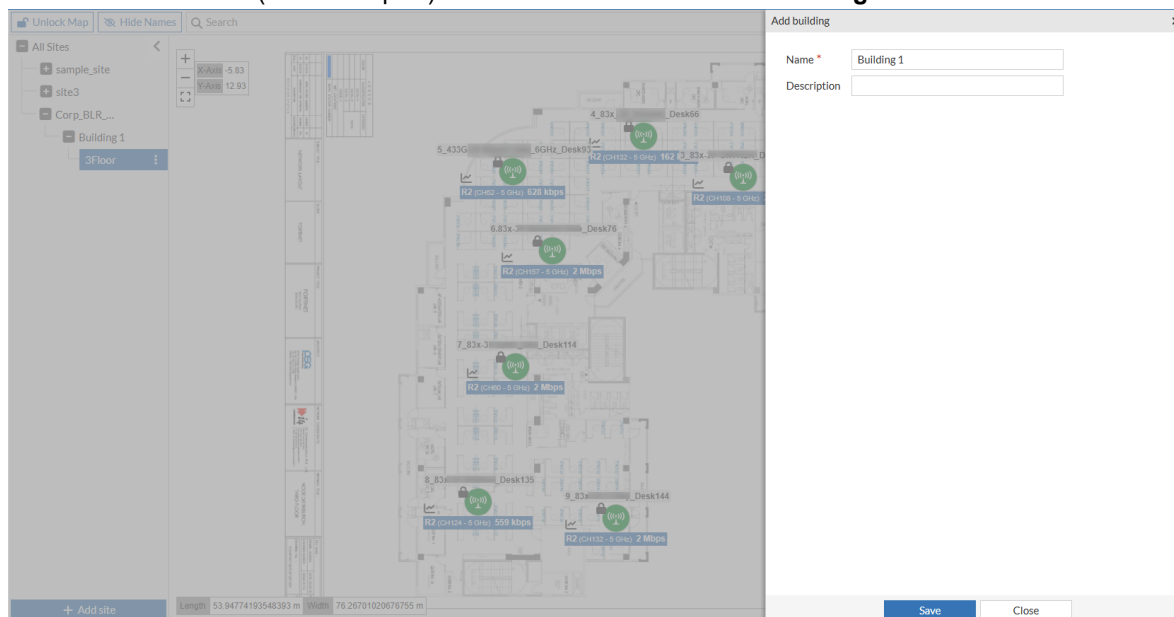
4. Click **Save**. The new site will appear in the left pane under **All Sites**.

Note: To delete a site, click the Kebab menu (vertical ellipsis) next to the site and click **Delete**. Deleting a site will delete the entire hierarchy contained within that site.

Adding a Building

A building is contained within a site and can have multiple floors.

1. On the left pane, select the site where you want to add a building.
2. Click the Kebob menu (vertical ellipsis) next to the site and click **Add Building**.



3. On the **Add building** pane, enter a **Name** and **Description**.
4. Click **Save**. The new building will appear under the selected site in the left pane.

Note: To delete a building, click the Kebob menu (vertical ellipsis) next to the site and click **Delete**. Deleting a building will delete the entire hierarchy contained within that building.

Adding a Floor

A floor is contained within a building and requires uploading a map image.

1. On the left pane, select the site and the building where you want to add a floor.
2. Click the Kebob menu (vertical ellipsis) next to the building and click **Add Floor**.
3. In the Floor Details section, enter a Name for the floor.

4. Upload the floor map file (must be in .jpg, .png, or .jpeg format).

Floor Details

Name: Floor_2

Image: map_floor_2.png 1.28 H x 1.18 W

Unit: ☐ Feet ☒ Meter

Drag two green pointer on floor map and position them across a known distance and enter the distance below. Based on this known distance, Floor Width and Length will be calculated automatically.

Selected Distance: 5

Dimension: 25 X 17.68

Image Preview

Cancel Save

5. Set the map scale:

- a. In the **Image Preview** section, drag the green pointer to two points on the map with a known distance between them.

Floor Details

Name: Floor_2

Image: map_floor_2.png 1.28 H x 1.18 W

Unit: ☐ Feet ☒ Meter

Drag two green pointer on floor map and position them across a known distance and enter the distance below. Based on this known distance, Floor Width and Length will be calculated automatically.

Selected Distance: 5

Dimension: 22.65 X 16.02

Image Preview

Cancel Save

- b. Under **Floor Details**, specify the **Unit** of measurement.
- c. Enter the actual distance between the two selected points in the **Selected Distance** field. The system automatically computes and displays the correct map scale in the **Dimension** field.
- d. Click **Save**. The new floor will appear under the selected site in the left pane.

Note: To delete a floor, click the Keobob menu (vertical ellipsis) next to the floor and click **Delete**. Deleting a floor will delete the entire hierarchy contained within that floor.

Importing and Exporting Maps

You can exchange **Wi-Fi Maps** with **EkaHau**, allowing you to import new maps and export modified ones for deeper analysis in the **EkaHau** application.

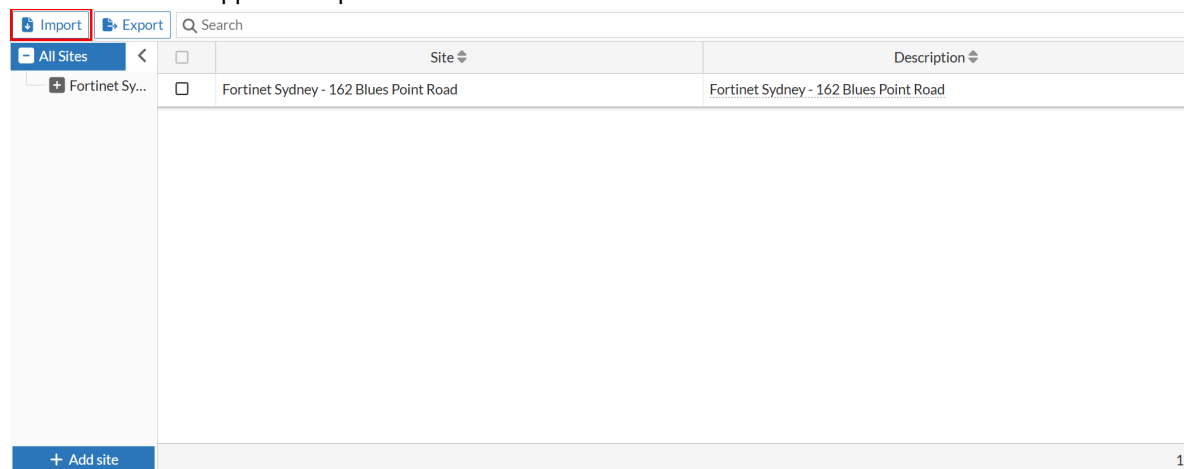
- [Importing Maps](#)
- [Exporting Maps](#)

Importing Maps

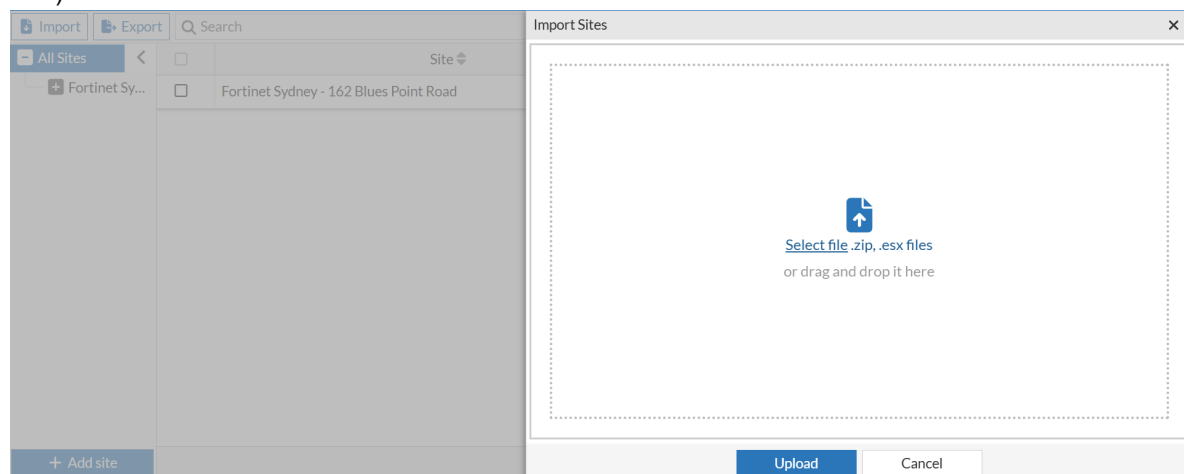
You can import maps created or modified in **EkaHau** directly into the system:

1. Navigate to **Wireless > Wi-Fi Maps**.
2. In the left pane, select **All Sites** or any site to import maps. Click **Import**.

Note: Maximum supported .zip or .esx file is 250 MB.



3. In the **Import Sites** pane, select your **EkaHau** file (either a .esx file or a .zip file containing multiple .esx files).



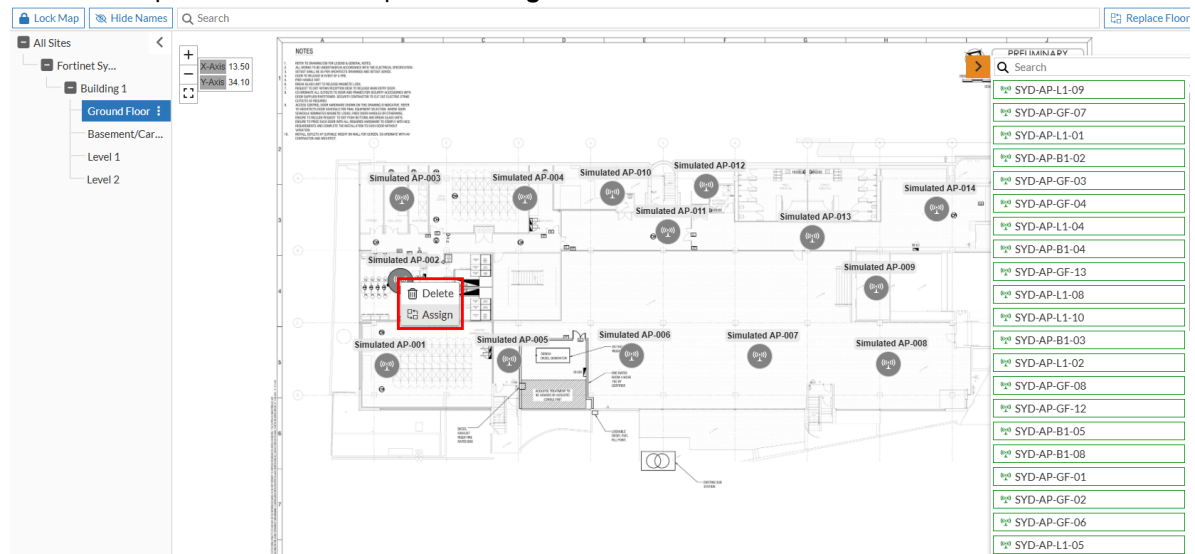
4. Click **Upload**.
The imported maps will appear in the left pane, structured appropriately.

Mapping APs

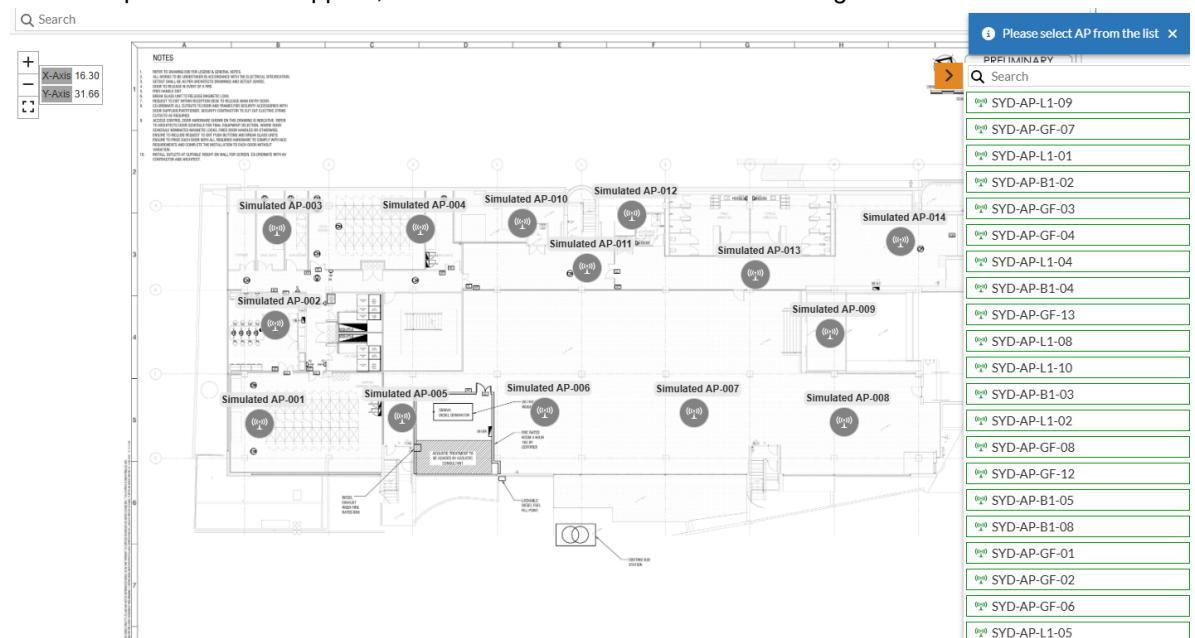
If the Access Point (AP) names in the imported map match your existing inventory names, the APs are mapped to their floor plan locations automatically.

If AP names do not match, those APs will be displayed in an **Inactive** state. To map them:

1. Click **Unlock Map**.
2. Select the unplaced AP on the map. Click **Assign**.



3. A list of unplaced APs will appear; select the correct AP from this list to assign it to the selected location.

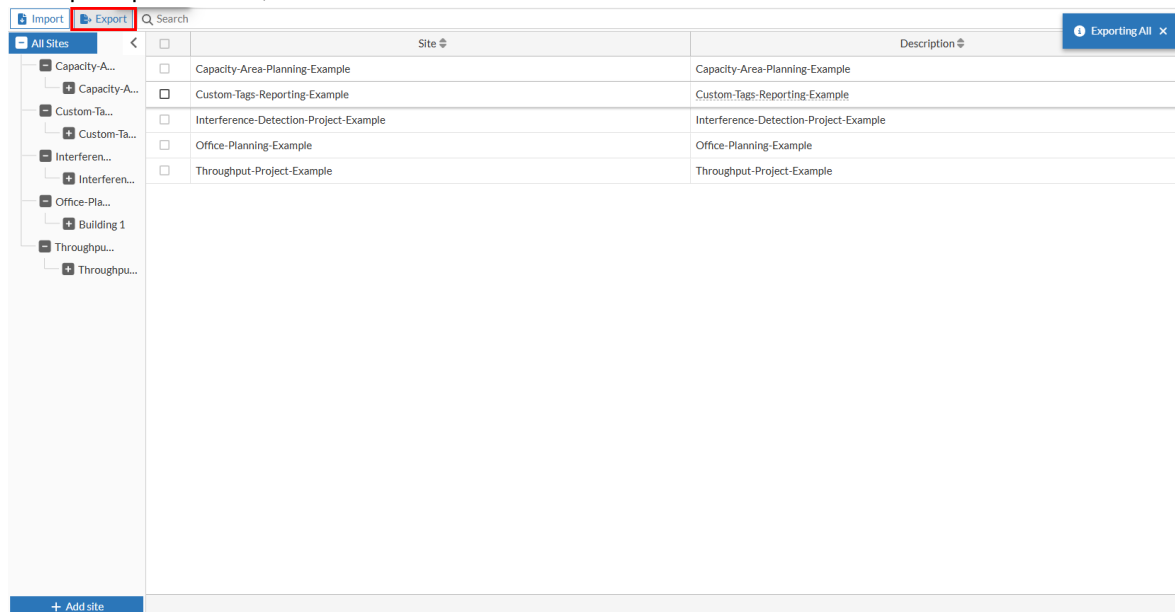


4. Click **Lock Map** when finished.

Exporting Maps

You can export modified maps and use them in **Ekahau** for further analysis.

1. Navigate to **Wireless > Wi-Fi Maps**.
2. To export all sites, select **All Sites**.
3. To export specific sites, use the check boxes to select the individual ones.



4. To export specific sites, use the check boxes to select the individual sites or navigate to the site (in the hierarchy) and click **Export**.
A .zip file containing the map(s) will be downloaded.

Modifying the Map

The **Unlock Map/Lock Map** options enables you to make any modifications to the floor map that is uploaded. You can make the following changes after you unlock a map:

- **Placing an Access Point** – when you unlock a map, the available APs are listed that can be placed on the map.
- **Replacing an Access Point** – replace an AP that is already added to a map with a different one.
- **Deleting an Access Point** – delete an AP that is added to the map.
- **Replacing a Floor Map** – replace the existing floor map with a different one.

Use the **Lock Map** option to save any changes made to the map during the **Unlock Map** phase.

Placing an Access Point

To place an AP on the floor map:

1. Navigate to the floor map and click **Unlock Map**.
2. On the right pane, a list of APs that are not placed is displayed.



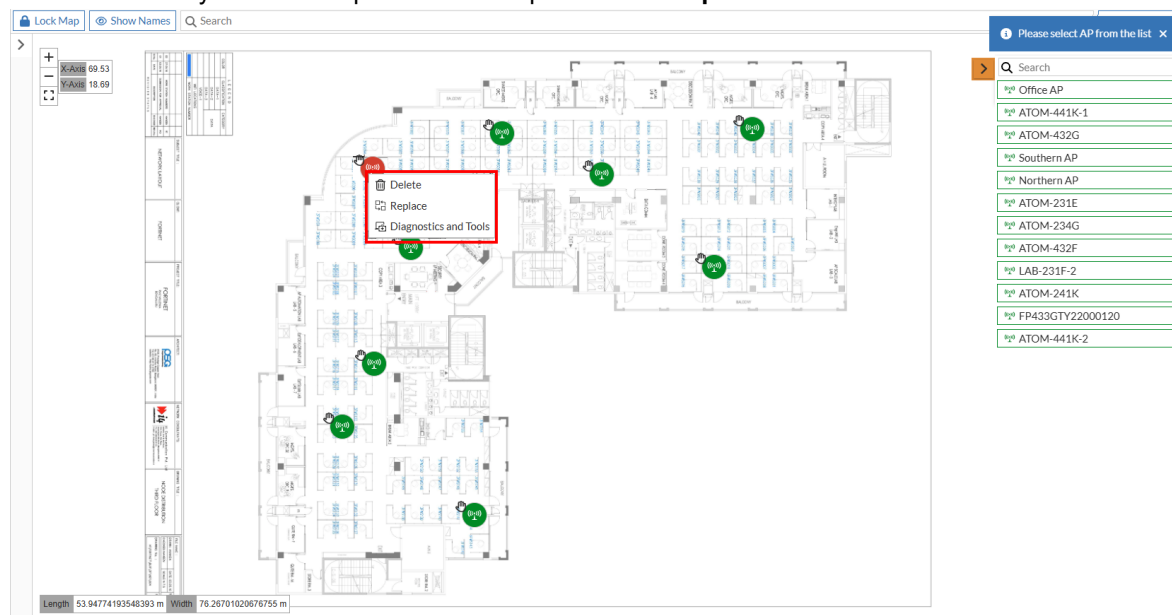
3. Drag and drop an AP at the desired location on the map.
4. Click **Lock Map** to save the changes.

Replacing an Access Point

To replace an existing AP with a different one on the floor map:

1. Navigate to the floor map and click **Unlock Map**.
2. On the right pane, a list of APs that are not placed is displayed.

- Click the AP that you want to replace on the map and select **Replace**.



- Select the required AP from the list. The AP selected on the map is replaced with the AP selected from the list.
- Click **Lock Map** to save the changes.

Deleting an Access Point

To delete an AP from a floor map:

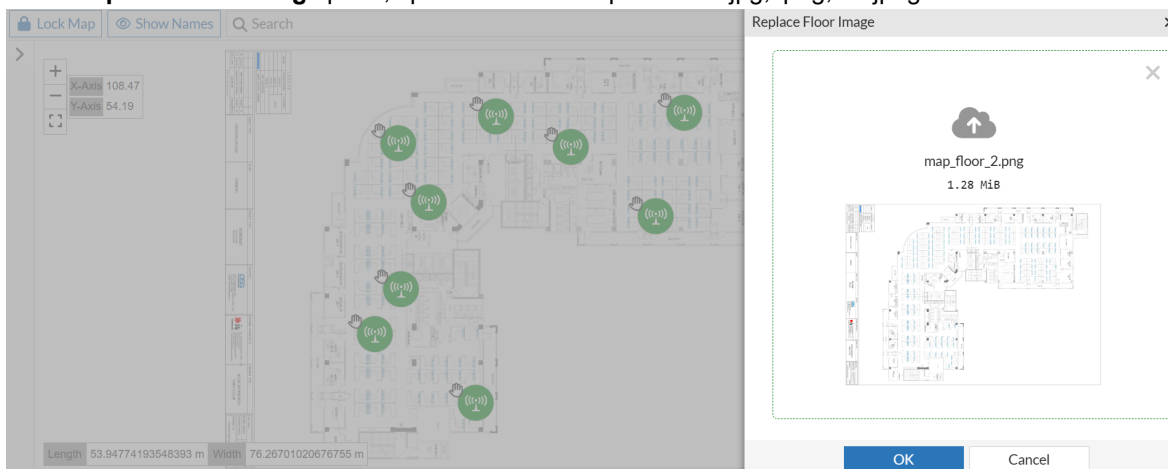
- Navigate to the floor map and click **Unlock Map**.
- Click the AP that you want to delete and select **Delete**.
The deleted AP is displayed on the **Unplaced Device(s)** list and can be re-used as necessary.
- Click **Lock Map** to save the changes.

Replacing a Floor Map

To replace a floor map:

- Navigate to the floor map and click **Unlock Map**.
- Click **Replace Floor**.

3. In the **Replace Floor Image** pane, upload the floor map in either .jpg, .png, or .jpeg format and click **OK**.



4. Click **Lock Map** to save the changes.

Viewing the Map

Wi-Fi Maps enables you to view the following details:

- [AP Status](#)
- [Show/Hide Names](#)
- [Search Bar](#)
- [Bands](#)
- [AP Stats](#)
- [Heatmaps](#)

AP Status

The status of an AP reflecting its connectivity is displayed on the map:

Online (Green)	The AP is currently active and connected.
Offline (Red)	The AP is currently disconnected or unreachable.
Inactive (Grey)	The AP is displayed on the map but is not actively managed by the current inventory. This state applies if: • The AP belongs to a Deleted FortiGate. • The FortiGate associated with the AP was moved from current ADOM to a different ADOM. • The AP was loaded using an Imported Map and its name does not match the AP names in the current ADOM's Access Point Inventory.

Show/Hide Names

Toggle the Hide Names and Show Names button to hide or display the customized names of the APs placed on the floor map.

Search Bar

The **Wi-Fi Maps** page features a global search bar that enables you to quickly locate devices and navigate through the map hierarchy. The following search types are supported:

- Site, Building, or Floor.
- AP Name or Serial Number.
- Device Name or Client MAC Address.

When a match is found, the map automatically navigates to the corresponding site, building, or floor and highlights the associated AP or client. This facilitates quick device location, placement review, and connectivity troubleshooting.

Refining your Search

If the search query does not immediately match a known Site, Building, or Floor, the system displays a prompt allowing you to refine the scope:

- Search for Client: Scans for connected clients by MAC address or device name, then navigates to the floor where the client is currently associated.
- Search for AP: Scans for APs by name or serial number and highlights them on the map.

Selecting one of these options restricts the search to the chosen category and displays the relevant results.

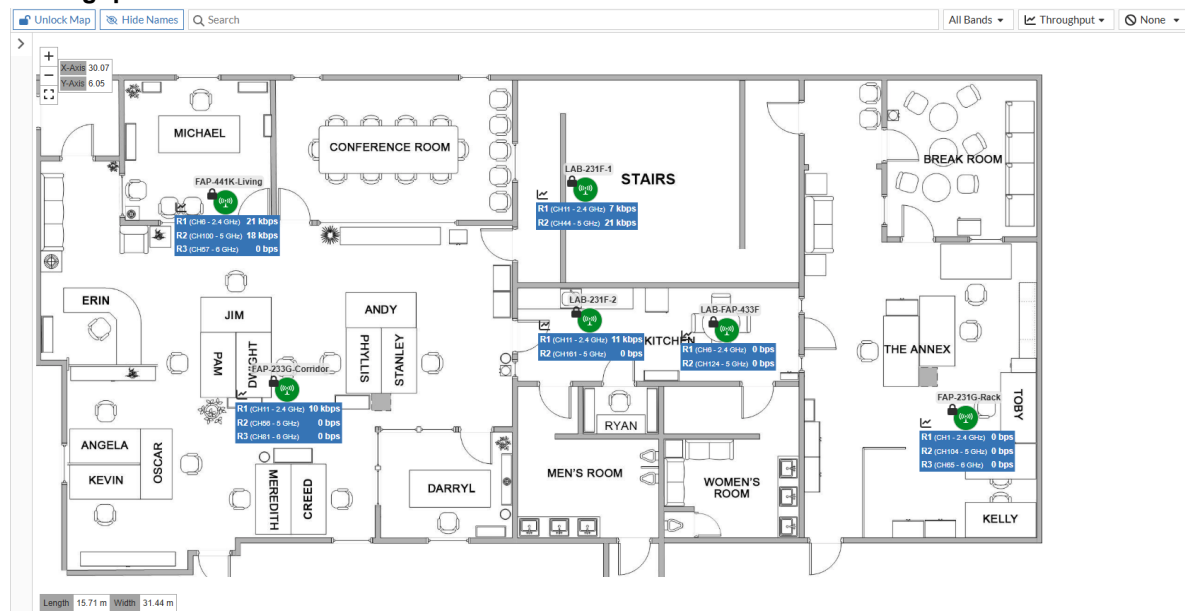
Bands

Bands filter the AP stats and Heatmaps data based on the specific band for the APs in the Inventory. This helps to visualize the AP distribution per frequency band.

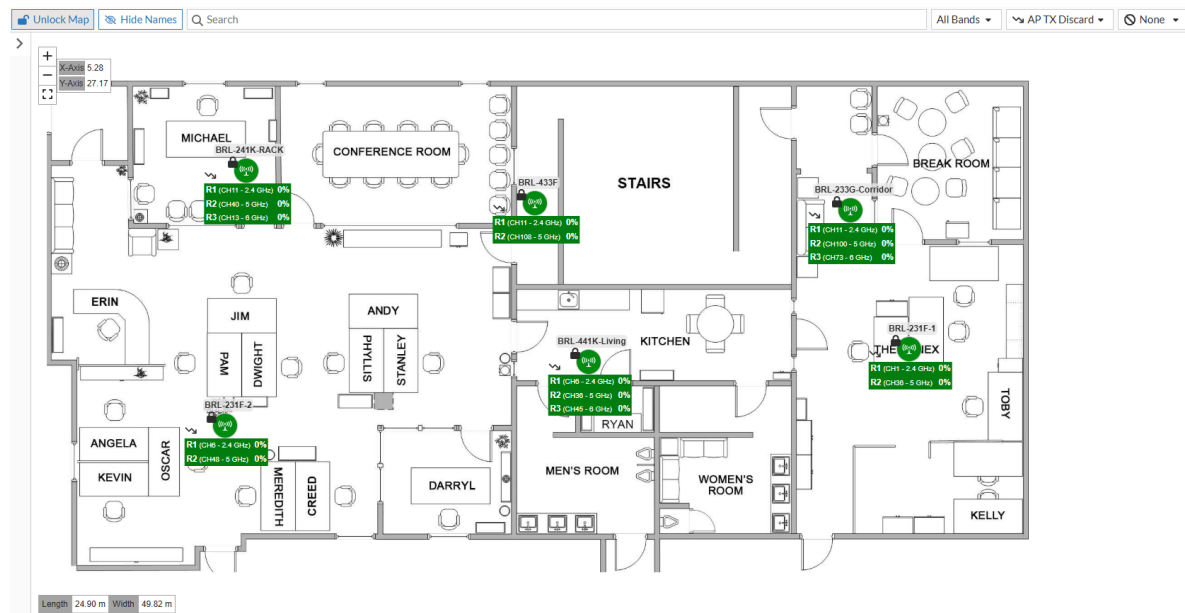
AP Stats

Select from the AP Stats drop-down menu to display real-time statistical data on the map for each AP. Available options include:

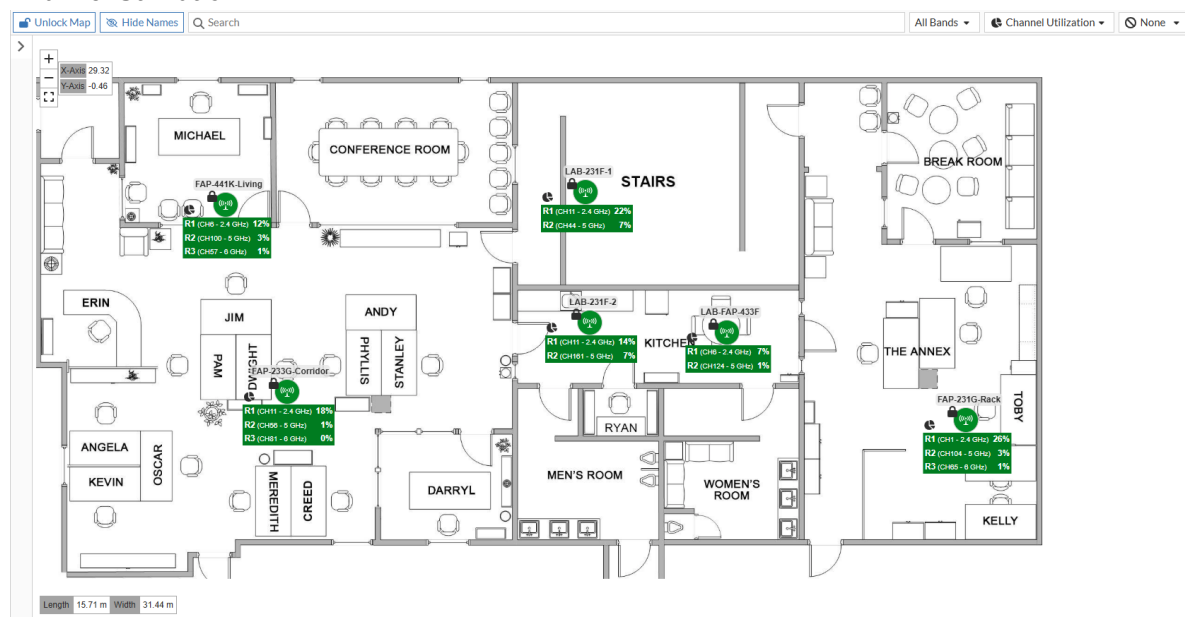
- **Throughput**



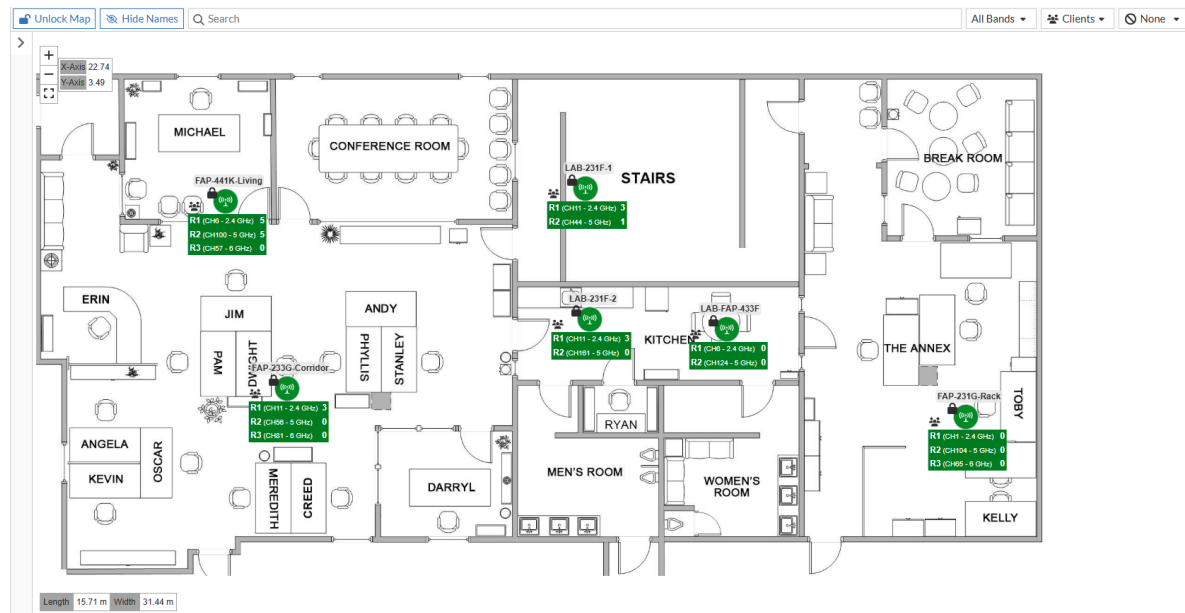
- **AP TX Discard**



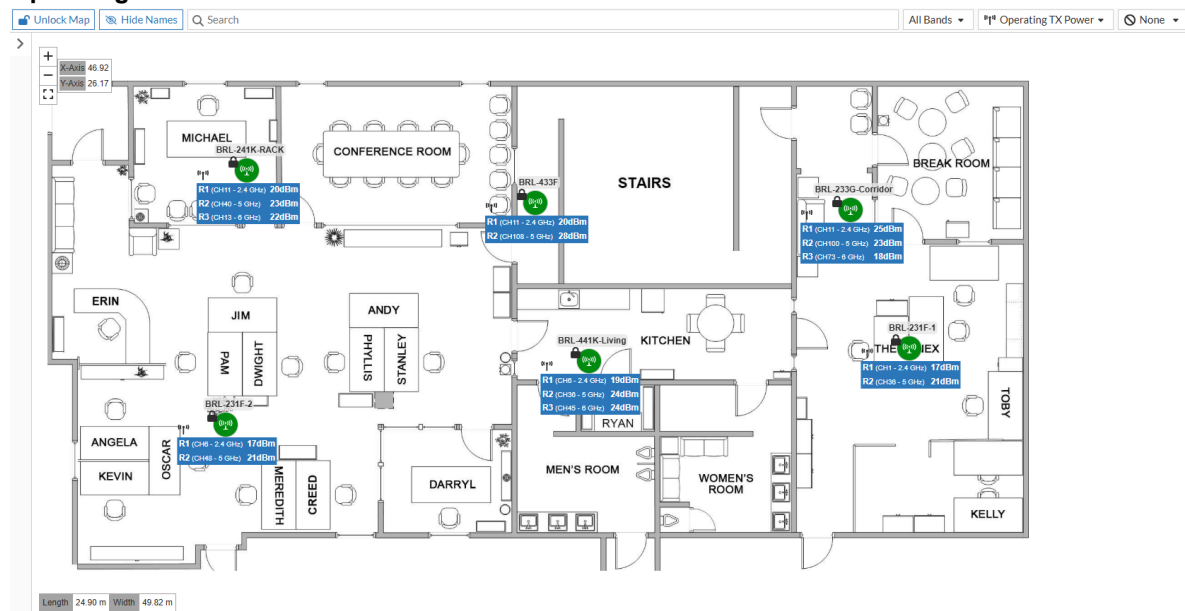
- **Channel Utilization**



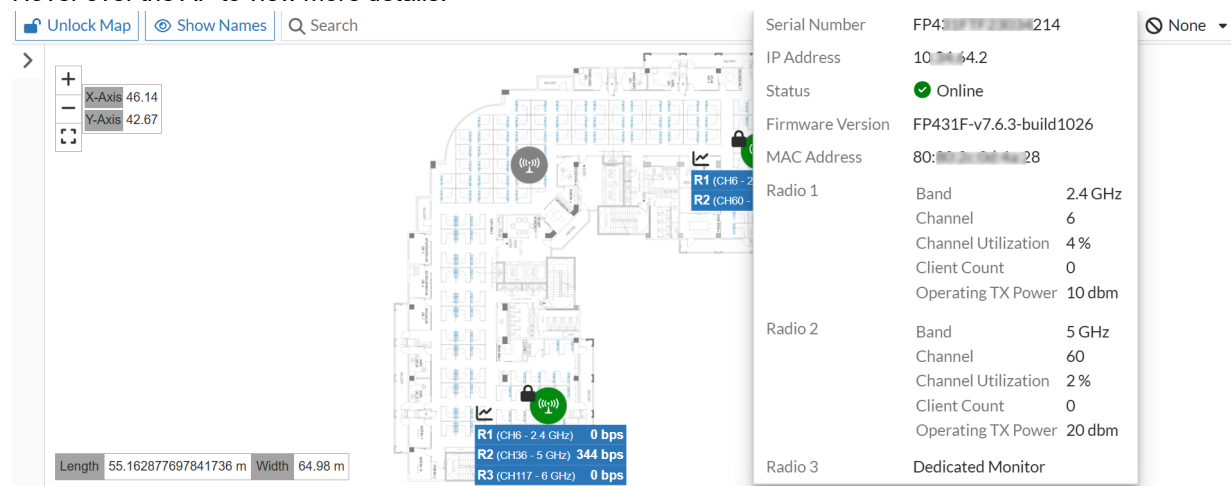
Clients



Operating TX Power



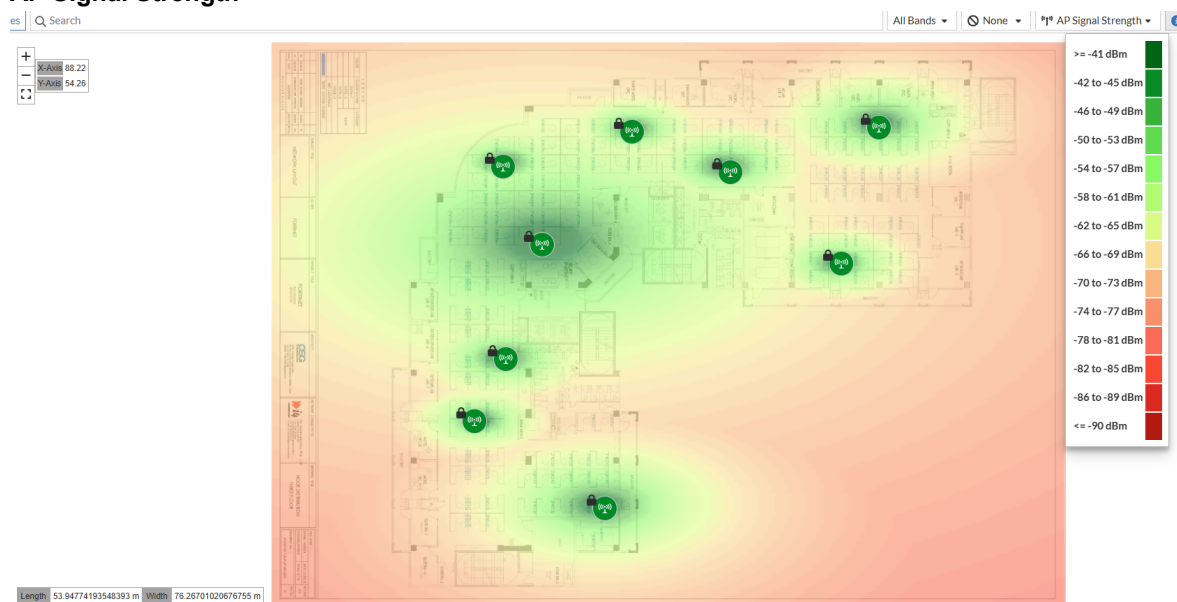
Hover over the AP to view more details.



Heatmaps

Select a value from the Heatmaps drop-down to visualize different metrics across the floor map using a color-coded representation (heatmap). Available heatmap values include:

- AP Signal Strength**



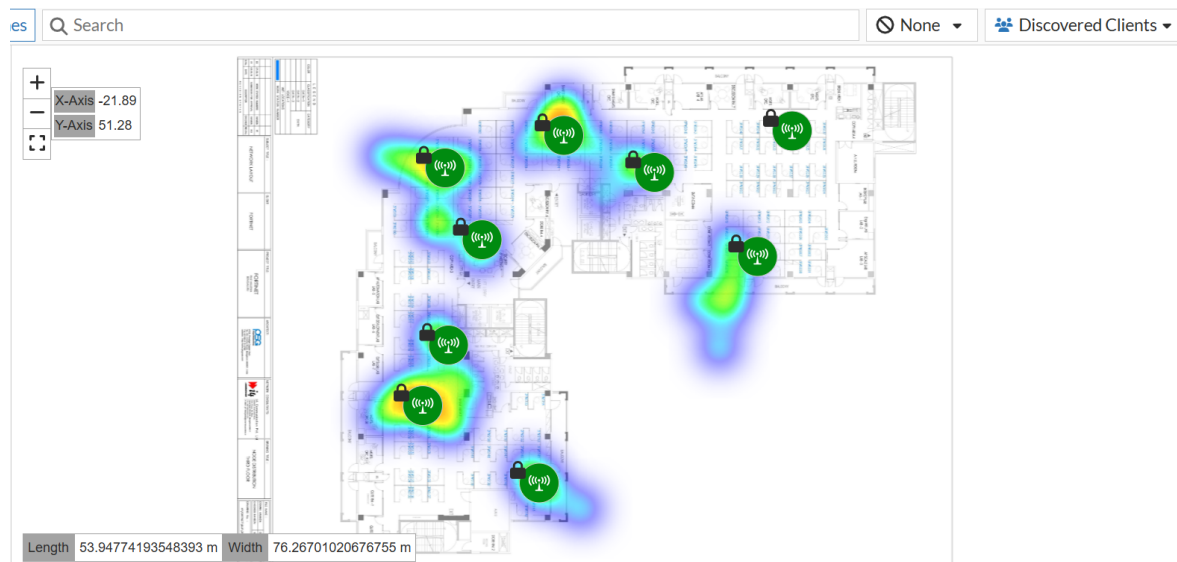
Hover over the  icon to see the legend explaining the colors used in the heatmap.

- **Connected Clients**



Click the **Filter** button to open the **Advanced Filters** pane. Use the options to narrow the list of connected clients. You can refine your search using the **Accuracy**, **OS Type**, and **Wireless Type** drop-down menus.

- **Discovered Clients**



- **Rogue APs**



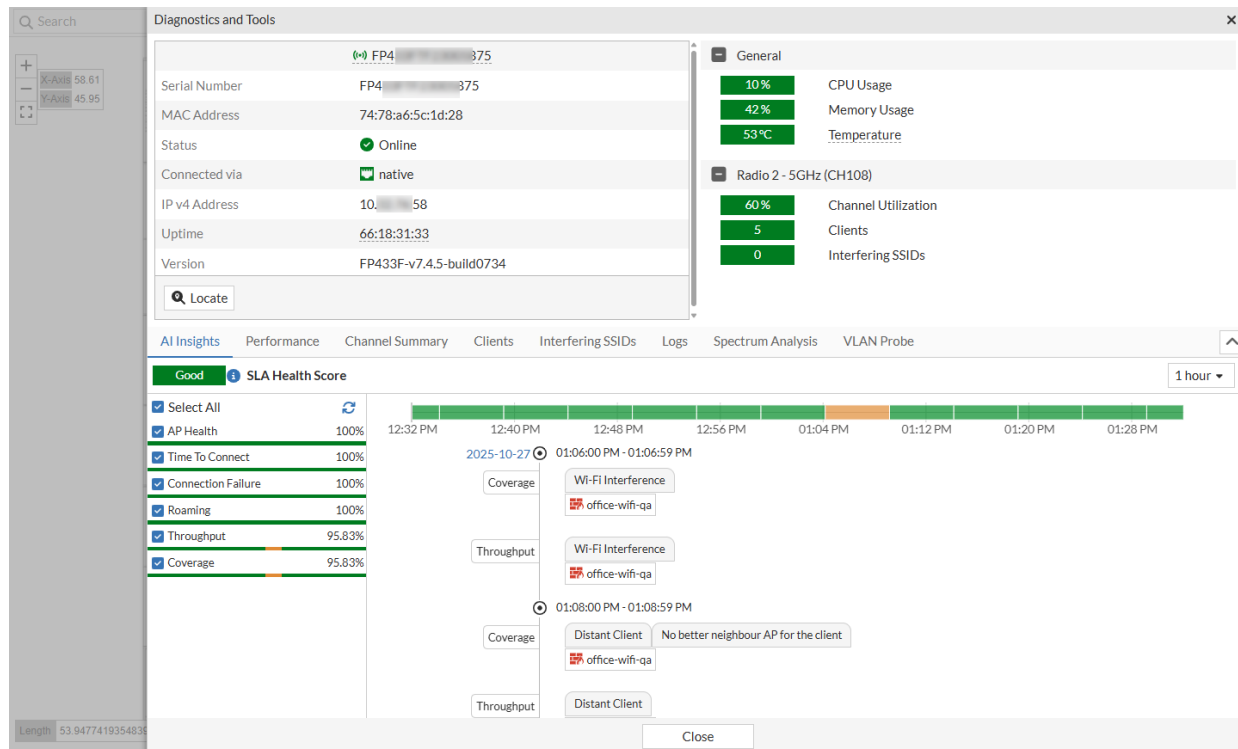
Diagnostics and Tools

The **Diagnostics and Tools** window provides detailed status information and allows you to run diagnostic tests for a selected Access Point. For information, see [Access Points Diagnostics and Tools](#).

To access the **Diagnostics and Tools** window, click on the required Access Point on the map and select **Diagnostics and Tools** from the options displayed.



The **Diagnostics and Tools** pane is displayed.



Note: The **Diagnostics and Tools** window is available in both **Unlock Map** and **Lock Map** modes.

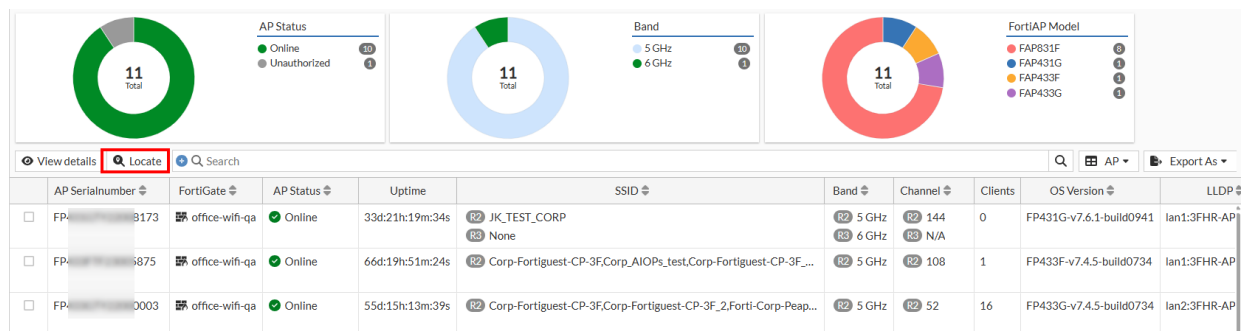
Locating Wireless Devices on the Map

The **Locate** feature across the wireless management screens enables you to quickly pinpoint the physical location of both Access Points (APs) and wireless clients on your network maps.

- [Locating Access Points \(APs\)](#)
- [Locating Wireless Clients](#)

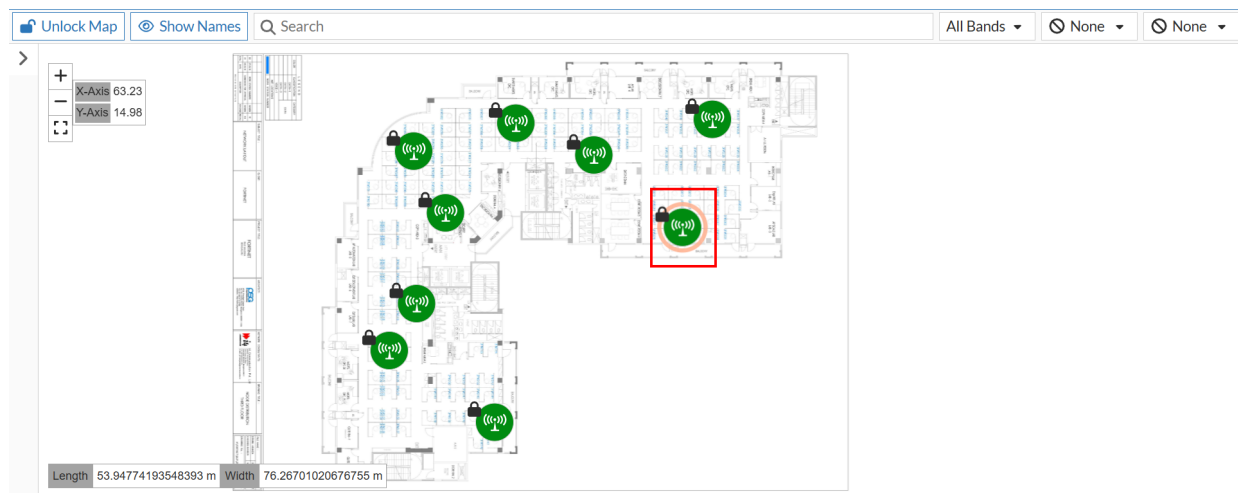
Locating Access Points (APs)

You can find the physical location of an AP from within the **Wireless > Access Points** window.

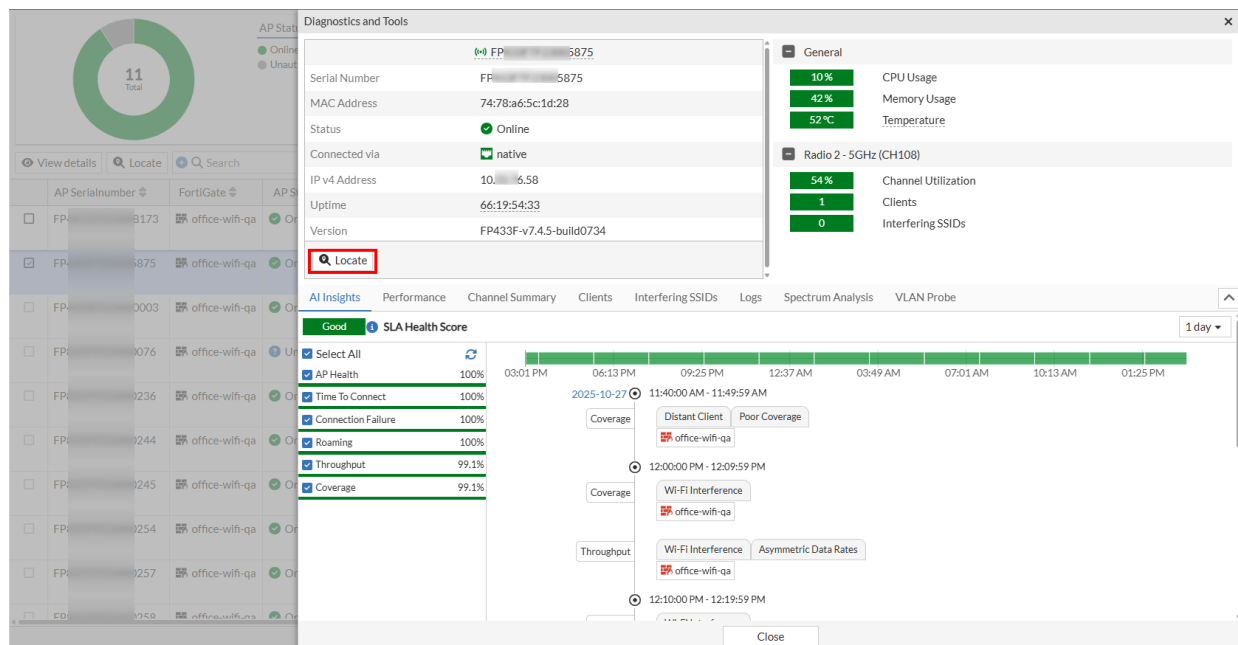


The device table includes a **Locate** option. Select an AP and click **Locate**.

The system opens the **Wi-Fi Maps** window to highlight the placement of the selected AP on its floor plan.



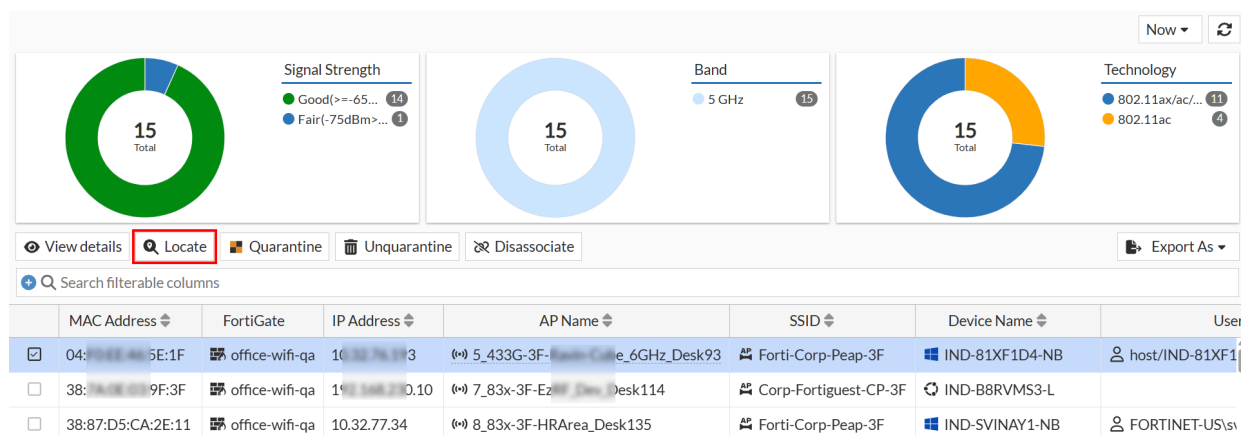
The **Diagnostics and Tools** pane has a dedicated **Locate** button. Clicking this button displays the map location of the currently selected AP within the **Wi-Fi Maps** window.



Locating Wireless Clients

The **Wireless > Wireless Clients** window also includes the locating capability.

The device table features a **Locate** option. Select any wireless client and click **Locate**.



The system opens the **Wi-Fi Maps** window and highlights the client's physical placement on the floor plan. The AP connected to the wireless client is also highlighted.

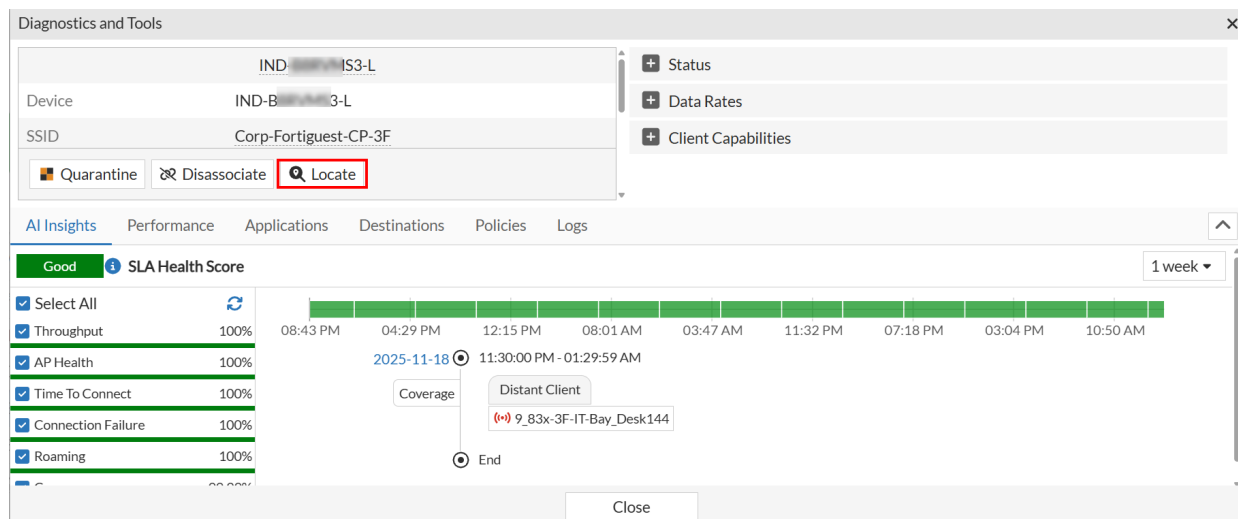


Clicking on the highlighted client will display its detailed information.



Right click on the client to display **Diagnostics and Tools** option for client.

Navigate to **Wireless > Wireless Clients** and select an individual client. Click **View Details**. This window displays the **Locate** button which can also be used to locate a client.



Clicking it shows the map location of the selected wireless client within the **Wi-Fi Maps** window.

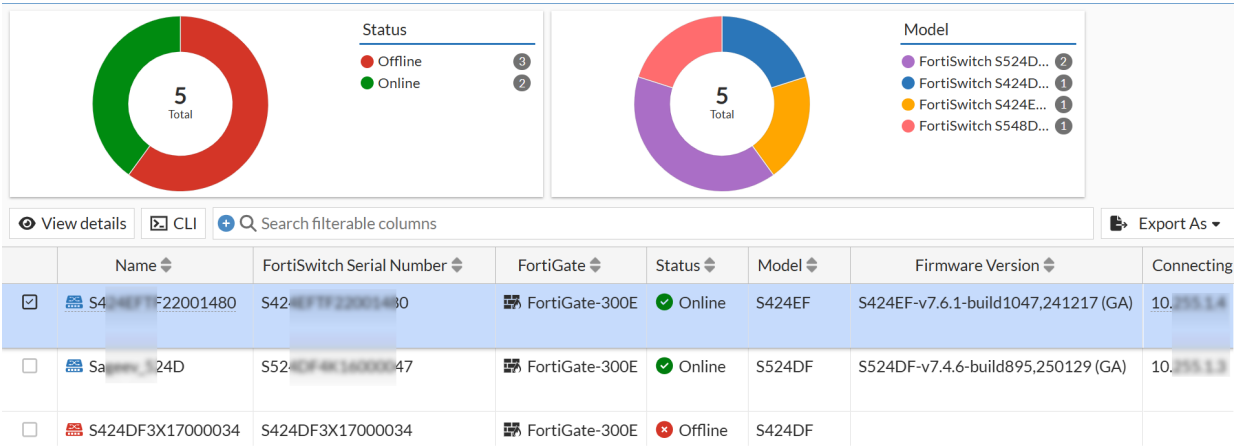
Switch

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

- [FortiSwitch](#)
- [Wired Clients](#)

FortiSwitch

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



Click **Export As** to export a table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.

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

- [FortiSwitch Diagnostics and Tools](#)

FortiSwitch 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

 S524DF-4K-1A0000047		General	
Name	S524DF-4K-1A0000047	6 %	CPU Usage
Serial Number	S524DF-4K-1A0000047	14 %	Memory Usage
Version	S524DF-v7.2.2-build419,220902 (GA)	7 day(s)	Connection Uptime
Model	S524DF	48° C	Temperature
		87 %	PoE Power Budget Remaining

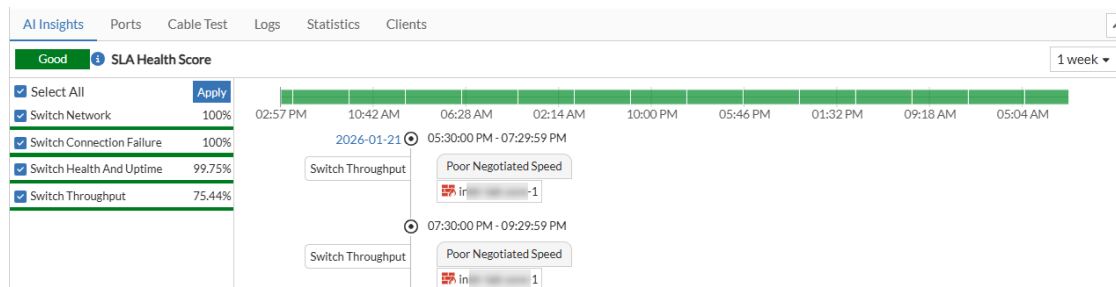
The following tabs are displayed:

- [AI Insights](#)
- [Ports](#)
- [Cable Test](#)
- [Logs](#)
- [Statistics](#)
- [Clients](#)

AI Insights

The **AI Insights** tab helps to analyze various performance metrics, identify issues, and provide detailed insights into the root cause of network problems, helping administrators maintain high service levels.

Note: This feature may not work as expected on Safari browser. For the best experience, use Chrome, Firefox, or Microsoft Edge instead.



The **SLA Health Score** provides the overall high-level score.

- **Good** for a score more 70
- **Fair** for a score between 30 and 70
- **Bad** for a score less than 30

Below the overall score, a list of individual SLAs or metrics is shown with their current health scores. You can select the SLAs that you want to track.

The following metrics are available:

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

When you click an SLA, the corresponding **SLA Summary** window opens with more details.

The bar graph (on the AI Insights tab) shows the performance trend over a selected time period (in this case, 1 week). The graph is divided to equal time segments. Based on the health score of each segment, the segments are colour coded as green (good), orange (fair), and red (bad).

Clicking on a specific time segment displays more details events that occurred during the time period.

Ports

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

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

Each entry in the port list displays the following information.

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

Cable Test

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

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

Diagnose		Search				Q
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

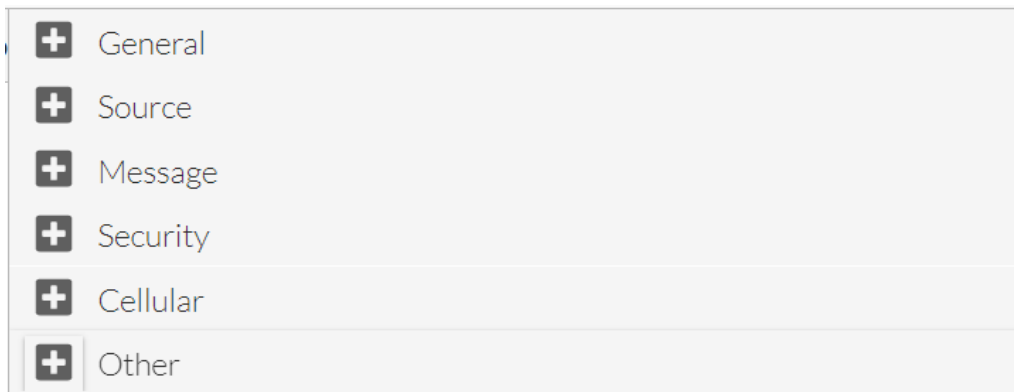
This tab displays the FortiSwitch log messages and the associated details.

Search		Q				Details
Date/Time	Level	Message	Log Description	Fortigate Serialnumber	FortiSw	
36 seconds ago	■ ■ ■ ■ ■ ■ ■ ■	primary port port19 instance 0 changed ...	FortiSwitch spanning Tree	FC148E181F0800	S524L	
38 seconds ago	■ ■ ■ ■ ■ ■ ■ ■	primary port port19 instance 0 changed ...	FortiSwitch spanning Tree	FC148E181F0800	S524L	
38 seconds ago	■ ■ ■ ■ ■ ■ ■ ■	primary switch port port19 has come up	FortiSwitch link	FC148E181F0800	S524L	
1 minute ago	■ ■ ■ ■ ■ ■ ■ ■	primary port port23 instance 0 changed ...	FortiSwitch spanning Tree	FC148E181F0800	S524L	

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.

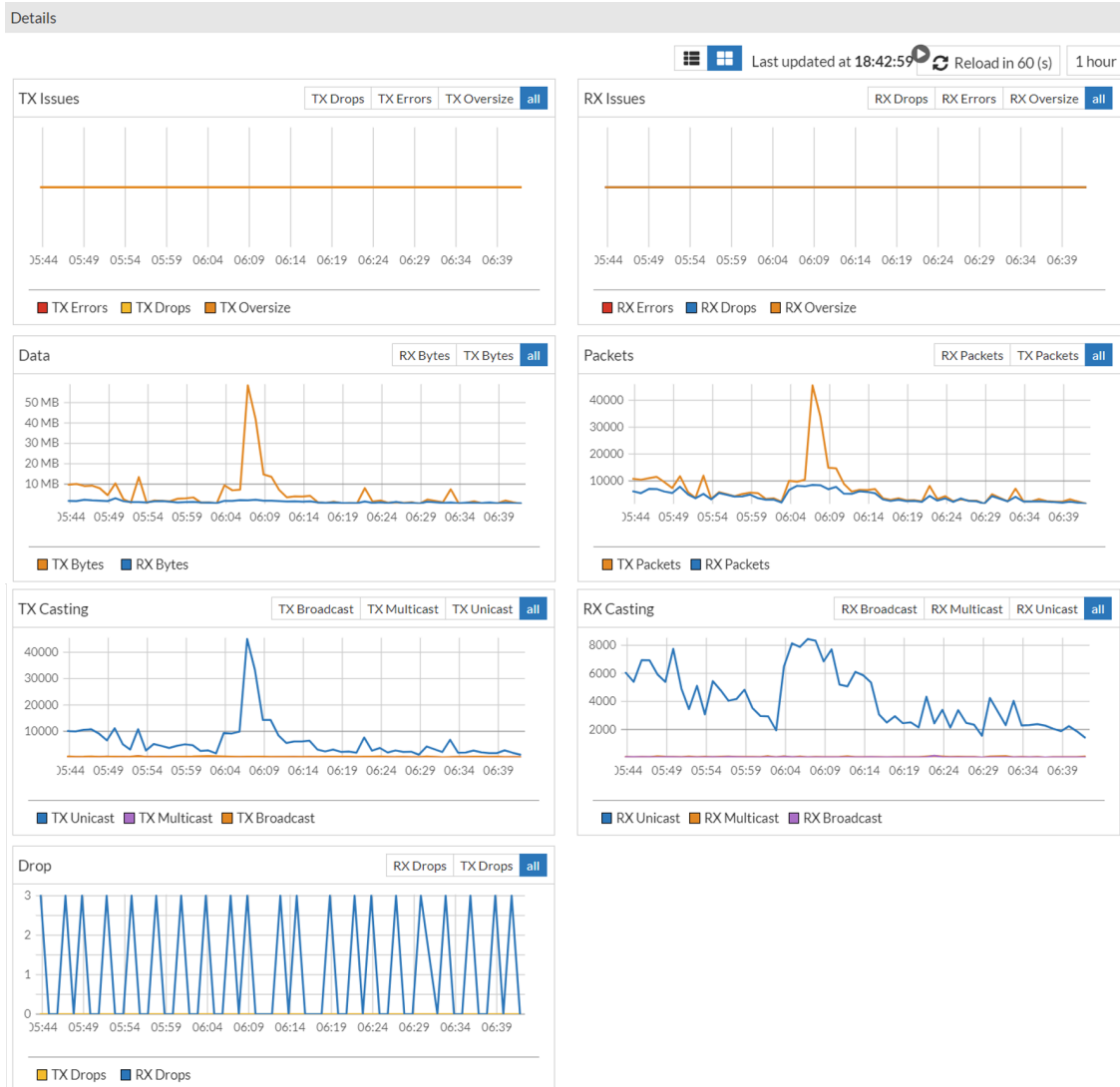
Ports		Switch				
View Trends		Search				
Port	TX Bytes	TX Packets	TX Unicast	TX Multicast	TX Broadcast	TX Errors
internal	1.62 GB	618,772,760	618,772,760	0	0	0
port1	3.56 GB	9,955,125	5,103,792	2,643,865	2,207,468	0
port2	215.61 MB	748,903	73,070	313,059	362,774	0

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

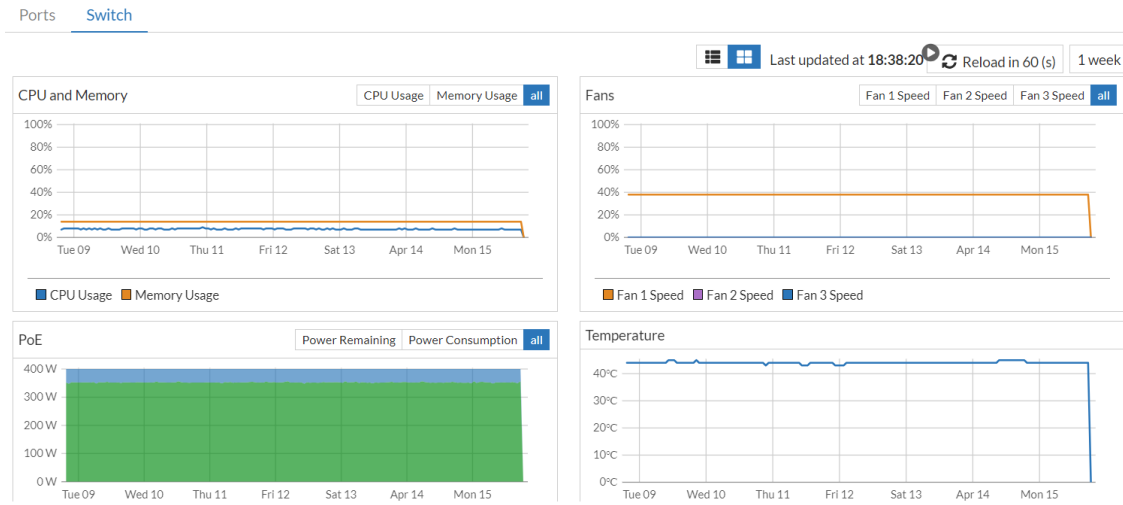
Parameter	Description
TX Bytes	The transmitted bytes.
TX Packets	The transmitted packets.
TX Unicast	The transmitted unicast packets.
TX Multicast	The transmitted multicast packets.
TX Broadcast	The transmitted broadcast packets.
TX Errors	The errors in transmitted packets.

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

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



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



Clients

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

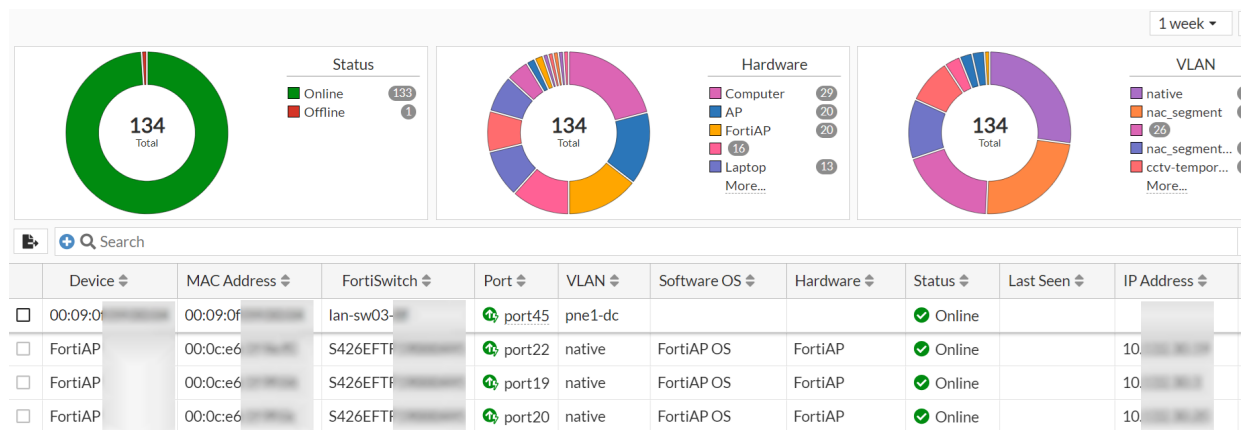
Parameter	Description
Device	The client device name.
Port	The associated port details.
VLAN	The associated VLAN details.
Software OS	The client device software OS.
Hardware	The client device hardware details.

Wired Clients

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

- You can filter the switching client data for a selected duration or a customized time slot. The **Custom range** allows the selection of a minimum of 1 hour and maximum of 1 week, the option of **Now** displays data for the last 1 minute.
- Click **Export As** to export a table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.

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



The table beneath the chart displays the client details.

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

FortiExtenders

The FortiExtenders window provides a comprehensive view for monitoring all FortiExtender devices across your network, including high-level summaries and in-depth diagnostics.

- [Extenders](#)

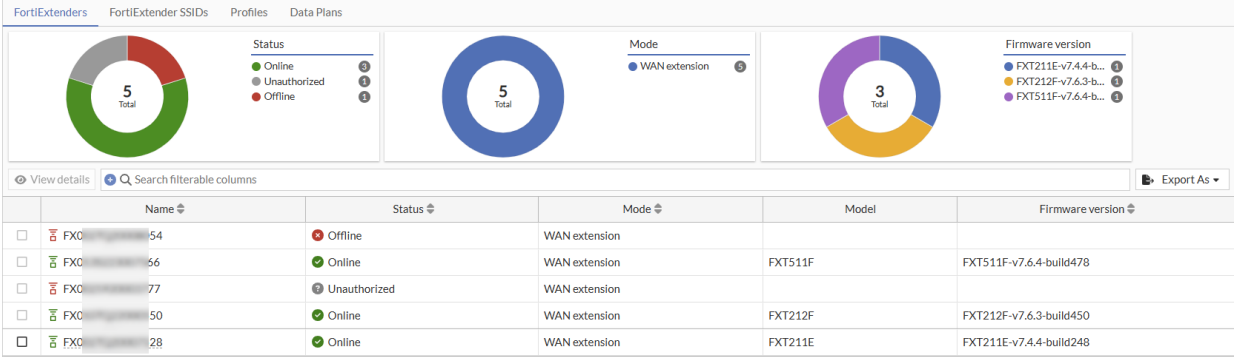
Extenders

The Extenders window is divided into the following tabs:

- [FortiExtenders](#)
- [FortiExtender SSIDs](#)
- [Profiles](#)
- [Data Plans](#)

FortiExtenders

The main **FortiExtenders** tab displays both visual summaries in the form of donut charts and a detailed device table.



Following charts are available:

- **Status:** Shows the total number of FortiExtenders that are Online versus Offline.
- **Mode:** Displays the number of devices based on their mode of operation: WAN extension mode or LAN extension mode.
- **Firmware Version:** Displays a count of devices grouped by their current firmware version.

The device table lists the following information for all FortiExtenders:

Name	Name of the FortiExtender
Status	Fortiextender status (online or offline)
Mode	Mode of operation (WAN extension or LAN extension)

Model	FortiExtender model
Firmware Version	FortiExtender firmware version
Data Usage	Current data usage
Details	FortiExtender details
ESN IMEI	FortiExtender electronic serial number (ESN) and international mobile equipment identity (IMEI)
FortiGate IP Address	IP address of FortiGate device
FortiGate Serial Number	Serial number of FortiGate device
ICCID	FortiExtender integrated circuit card identity (ICCID) number
IMSI	FortiExtender international mobile subscriber identity (IMSI) number
IP Address	FortiExtender IP address
Modem 1 interface	Name of the Modem 1 Interface
Modem 2 Interface	Name of the Modem 2 Interface
Network	FortiExtender carrier name
Phone Number	FortiExtender phone number
Profile	Profile name of the FortiExtender
RSRP	The Reference Signal Received Power
RSRQ	The Reference Signal Received Quality
RSSI	The Received Signal Strength Indicator
Serial Number	Serial number of the FortiExtender
SINR	The Signal-to-Interference-plus-Noise Ratio
Temperature	Temperature information of FortiExtender
VDOM	Virtual domain

The **Export As** option enables you to export the table data (filtered or all data) in formats like CSV, JSON, Plaintext, or PDF.

Note: You can customize the exported data by selecting up to 8 columns to include in the file.

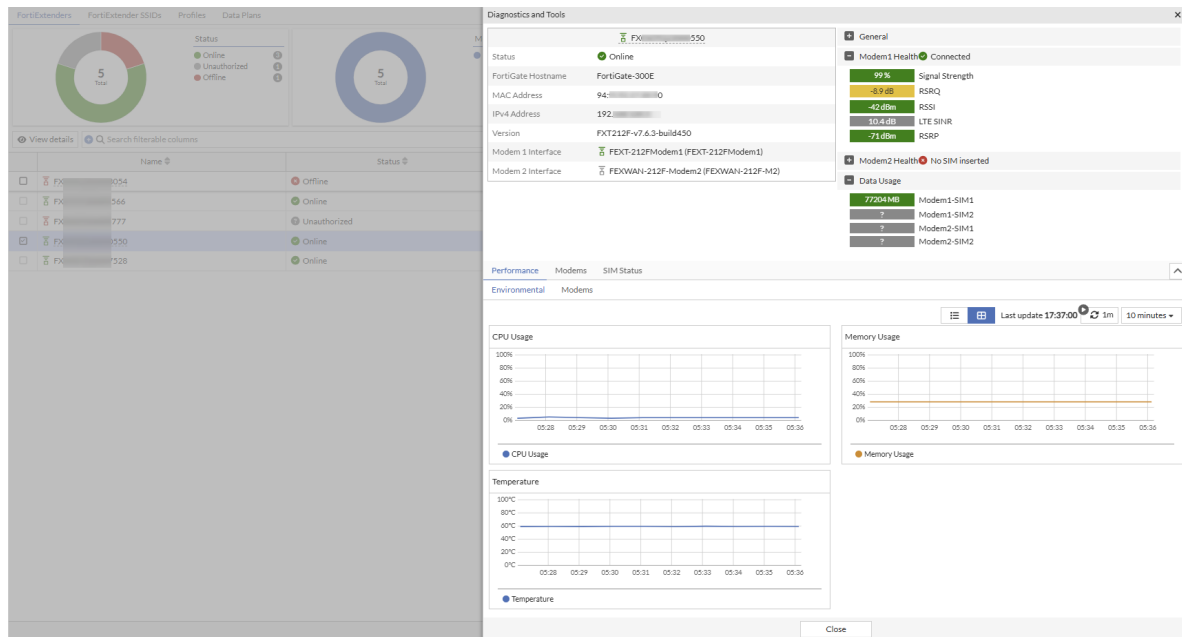
To access detailed statistics and troubleshoot a device, select a FortiExtender from the table and click **View Details**. This opens the **Diagnostics and Tools** pane, which contains the following tabs:

- [Performance](#)
- [Modems](#)
- [SIM Status](#)

Performance

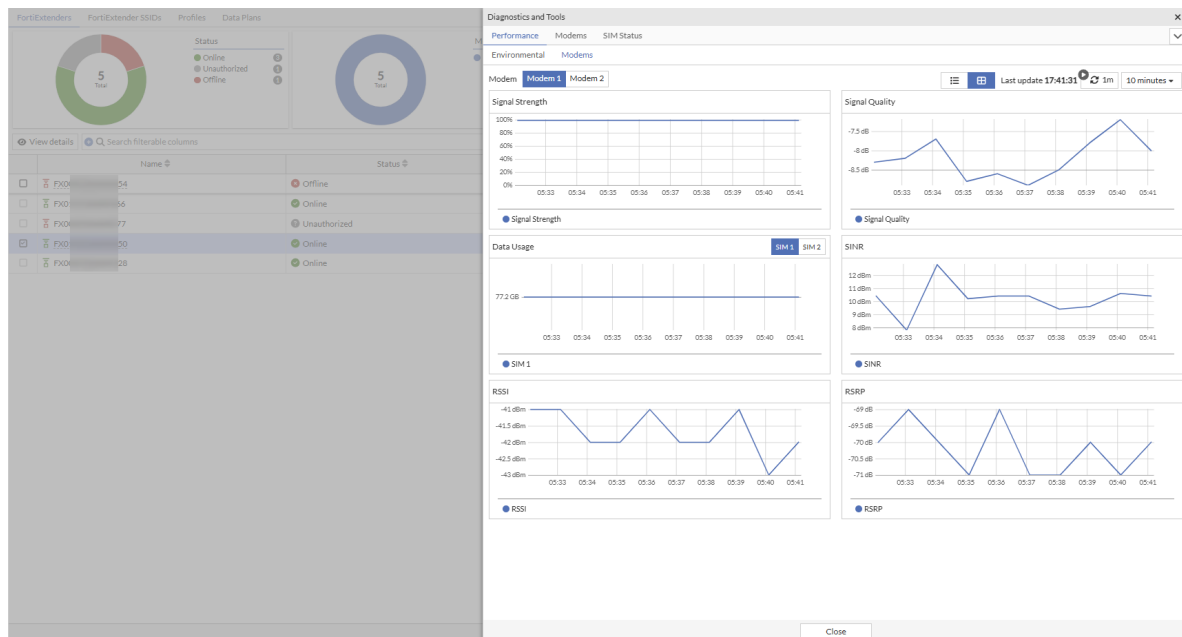
This tab displays charts tracking the FortiExtender's health and usage:

- **Environmental:** The Environmental sub-tab provides critical charts detailing the FortiExtender's environmental and resource health over the specified time period.



The following charts are available:

- CPU Usage
- Memory Usage
- Temperature
- **Modems:** The Modems sub-tab provides critical performance metrics for both Modem 1 and Modem 2 over a specified time period.



These details are presented through individual charts for each of the following

- Signal Strength
- Signal Quality
- Data Usage
- SINR (Signal-to-Interference-plus-Noise Ratio)
- RSSI (Received Signal Strength Indicator)
- RSRP (Reference Signal Received Power)

Modems

The screenshot shows the FortiExtenders web interface. On the left, a donut chart indicates 5 total devices, with 2 offline (red) and 3 online (green). The main panel is titled 'Diagnostics and Tools' and shows details for a selected modem (FX010). The details include Name, Status (online), FortiGate Hostname, MAC Address, IPv4 Address, Version, Modem 1 Interface, and Modem 2 Interface. Below the details, there are tabs for Performance, Modems, and SIM Status. The Modems tab is active, showing a table of all modems.

Modem	Status	Manufacturer	Model	Service	Assigned Data Plan
Modem1	Online	Sierra Wireless, Incorporated	EM7565	LTE	
Modem2	Offline	Sierra Wireless, Incorporated	EM7565		

This tab provides key hardware and configuration details for the FortiExtender's modems. Details such as Status, Manufacturer, Assigned Data Plan, Service, and Model of the modems are displayed.

SIM Status

The screenshot shows the FortiExtenders web interface. On the left, a donut chart indicates 5 total devices, with 2 offline (red) and 3 online (green). The main panel is titled 'Diagnostics and Tools' and shows details for a selected modem (FX010). The details include Name, Status (online), FortiGate Hostname, MAC Address, IPv4 Address, Version, Modem 1 Interface, and Modem 2 Interface. Below the details, there are tabs for Performance, Modems, and SIM Status. The SIM Status tab is active, showing a table of SIM status for both Modem1 and Modem2.

SIM Slot	Status	Carrier	Phone Number	Switch Status	Data Usage	IMSI	ICCID
Modem1							
SIM 1	Inserted	airtel		Active	77203 MB	40-615	899-737
SIM 2	Not Inserted			Backup	0 MB	N/A	
Modem2							

The **SIM Status** tab displays details for the cellular Subscriber Identity Modules (SIMs) in the modems. The information displayed for each SIM includes Status, Carrier, Phone Number, Switch Status, Data Usage, IMSI, and ICCID related to both SIM 1 and SIM 2 of the Modems available.

FortiExtender SSIDs

FortiExtenders								
<u>FortiExtender SSIDs</u>		Profiles	Data Plans					
Search Q Export As ▾								
	Name 📎	SSID 📎	Type 📎	Security 📎	FortiGate IP Address 📎	FortiGate Serial Number 📎	VDOM 📎	IP/Netmask
☐	Ext_Tunnel	Ext_Tunnel(1_Ext_Tunnel)	local-vap	WPA2-Personal	10.10.10.10	FG31A0000000083	root	30.30.30.24
☐	Ext_test	Ext_test(A_ext_test)	lan-ext-vap	WPA2-Personal	10.10.10.10	FG11A0000000056	root	0.0.0.0
☐	Ext	Ext()	local-vap	OPEN	10.10.10.10	FG31A0000000083	root	0.0.0.0
☐	Ext_ext	Ext_ext(local_ext)	local-vap	WPA2-Personal	10.10.10.10	FG11A0000000056	root	0.0.0.0
☐	Ext2	Ext2()	local-vap	WPA2-Personal	10.10.10.10	FG31A0000000083	root	1.1.1.1

This tab lists SSID configuration details, including Name, SSID, Type, Security, FortiGate IP Address, FortiGate Serial Number, VDOM, and IP/Netmask.

Profiles

FortiExtenders

FortiExtender SSIDs

Profiles

Data Plans

Model

- FX211E 6
- FX201E 5
- FX212F 3
- FVG22F 2
- FX511F 2
- More...

Mode

- WAN extension 15
- LAN extension 7

	Name	Model	Mode	FortiGate IP Address	FortiGate Serial Number	VDOM
☐	FEV212F	FVG22F	LAN extension	192.168.1.1	FGT1234567890123456	root
☐	FEXT_22F	FVG22F	WAN extension	192.168.1.1	FGT1234567890123456	root
☐	FX211E-lanext-default	FX211E	LAN extension	192.168.1.1	FGT1234567890123456	root
☐	FX211E-wanext-default	FX211E	WAN extension	192.168.1.1	FGT1234567890123456	root
☐	FX511F-lanext-default	FX511F	LAN extension	192.168.1.1	FGT1234567890123456	root
☐	FX511F-wanext-default	FX511F	WAN extension	192.168.1.1	FGT1234567890123456	root

This tab displays information about configuration profiles, such as Name, Model, Mode, FortiGate IP Address, FortiGate Serial Number, and VDOM.

Data Plans

FortiExtenders											
FortiExtender SSIDs		Profiles		Data Plans							
Q Search											Export As ▾
☐	Name ☼	Modem ☼	Carrier ☼	APN ☼	Capacity ☼	Monthly Cost ☼	Billing Date ☼	Type ☼	FortiGate IP Address ☼	FortiGate Serial Number ☼	VDOM ☼
☒	S- [REDACTED]	all			50,000	0	1	generic	10.0.0.1	FG-[REDACTED]-6	root
☐	D- [REDACTED]	modem1	jionet	jionet1	100	0	1	carrier	10.0.0.110	FG-[REDACTED]-83	root
☐	Jc- [REDACTED]	all		jionet	0	0	1	iccid	10.0.0.142	FG-[REDACTED]-44	root
☐	N- [REDACTED]	modem1		airtel.net	2,000	0	1	generic	10.0.0.110	FG-[REDACTED]-83	root
☐	Pf- [REDACTED]	modem1	airtel	airte.net	0	0	1	carrier	10.0.0.110	FG-[REDACTED]-83	root
☐	f- [REDACTED] DP	all			0	0	1	generic	10.0.0.142	FG-[REDACTED]-44	spaltest

This tab shows all configured cellular data plans, including Name, Modem, Carrier, APN, Capacity, Monthly Cost, Billing Date, Type, FortiGate IP Address, FortiGate Serial Number, and VDOM.

SD-WAN

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



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

- [Prerequisites](#)
- [Recommendations](#)

Prerequisites

The following configurations are necessary to enable proper monitoring:

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

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

For more details, see [FortiGate Administration Guide](#).
- Enable Application Control to ensure accurate computation of SD-WAN traffic, along with detailed reporting of SD-WAN rule utilization, application usage, and bandwidth consumption. For more information, see [FortiGate Administration Guide](#).

Recommendations

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

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

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

- [Insights](#)
- [Forecast](#)

Insights

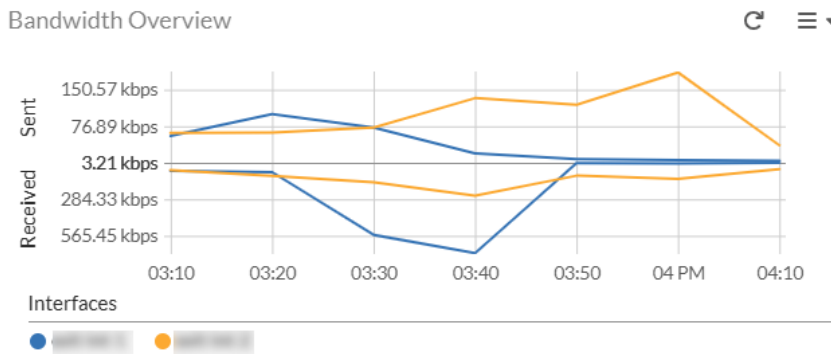
The Insights page provides valuable insights into your network's health and performance with the charts:

- [Bandwidth Overview](#)
- [Available Bandwidth](#)
- [Used Bandwidth](#)
- [Performance Status](#)
- [Rules Utilization](#)
- [Applications Utilization](#)
- [MOS Score](#)
- [SLA Performance Issues](#)

Bandwidth Overview

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

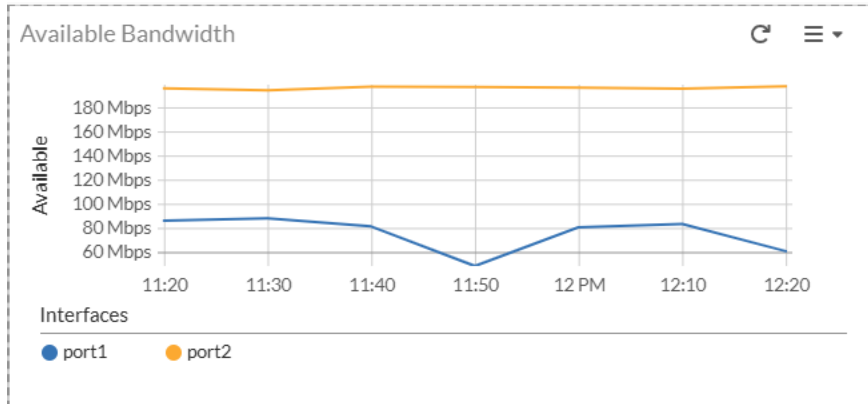
Hover over the points on graph to view sent/receive data.



Available Bandwidth

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

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

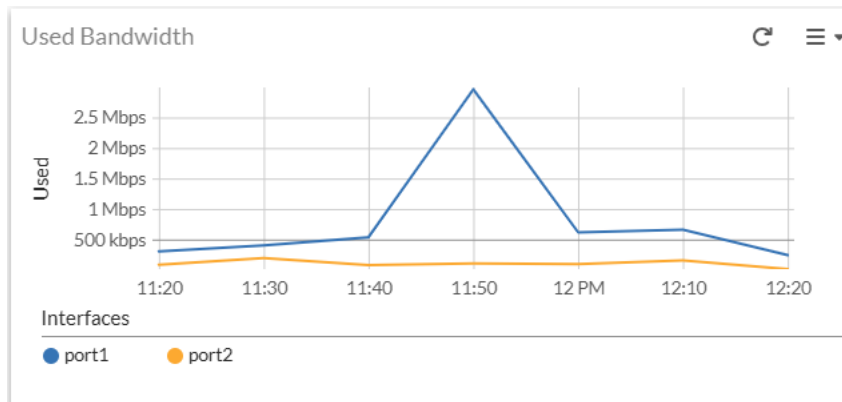


Note: Configure **Estimated Bandwidth** to estimate accurate WAN utilization. If not configured, the maximum capacity of the link is inserted as **Available Bandwidth**. For more information, see [FortiGate Administration Guide](#).

Used Bandwidth

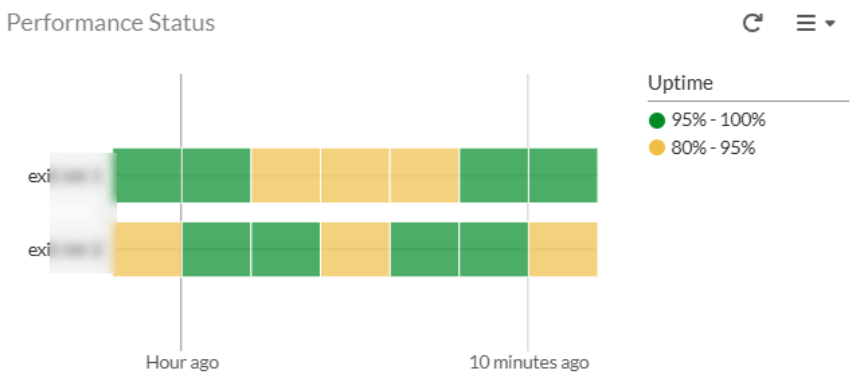
This chart displays the amount of bandwidth consumed by the SD-WAN interfaces over a period of time.

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



Performance Status

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



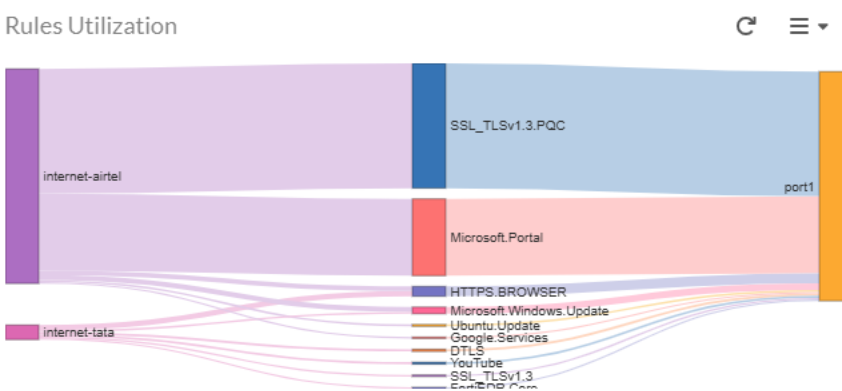
Color-coded indicators represent uptime percentages:

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

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

Rules Utilization

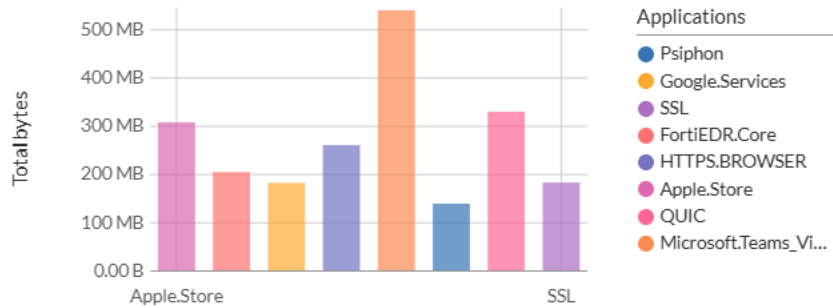
This chart shows how SD-WAN rules, which govern traffic routing across SD-WAN interfaces, are utilized. It presents a detailed view of traffic distribution, displaying data for both the interface through which the traffic flows and the applications generating the traffic. Hover your cursor over the data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



Applications Utilization

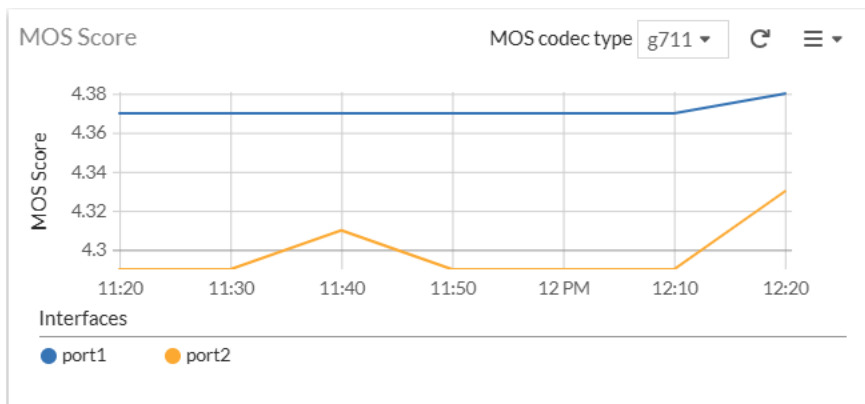
This chart displays a detailed overview of bandwidth consumption, showing the top 10 applications and their respective bandwidth distribution across the configured SD-WAN interfaces. Hover your cursor over the data points for a more detailed information.

Applications Utilization



MOS Score

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



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

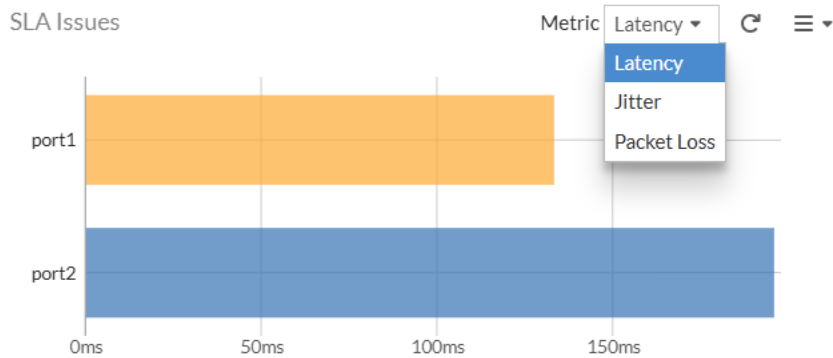
- MOS 4.3-5.0: Excellent
- MOS 4.0-4.3: Good
- MOS 3.6-4.0: Fair
- MOS 3.1-3.6: Poor
- MOS 2.6-1.0: Bad

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

SLA Performance Issues

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

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



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

Forecast

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

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

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

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

- [Configure Baselines](#)
- [Performance Summary](#)
- [Health Check Trends](#)
- [Anomalies](#)

Configure Baselines

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

Manage Baseline

Choose Baseline computation mode.

☐ Static Baseline 

Select for fixed baseline settings sourced from FortiGate

☒ Dynamic Baseline 

Select for adaptive baseline settings that change dynamically every week

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

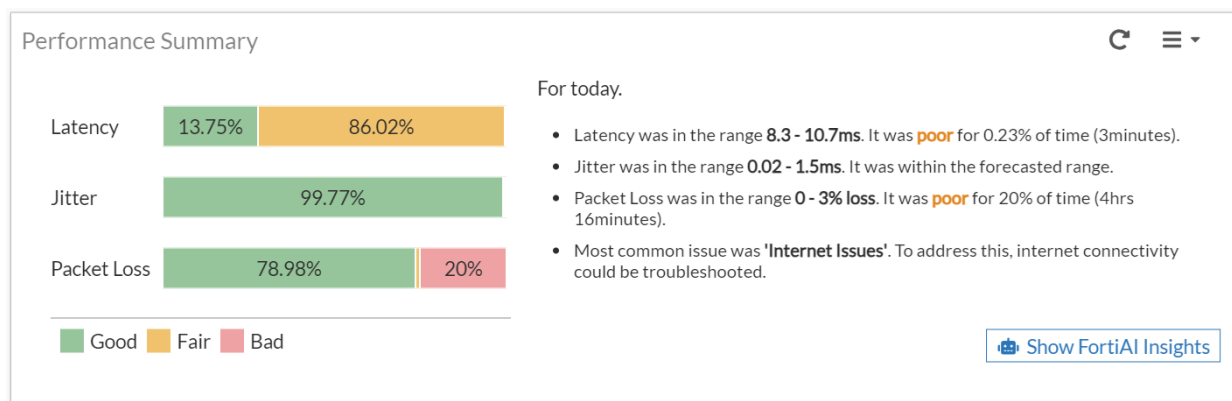
- Latency - 100 ms
- Jitter - 30 ms
- Packet Loss - 1 %

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

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

Performance Summary

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



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

 FortiAI Insights (1)

Interested in knowing more about SD-WAN performance prediction?

What are the most common issues on the selected interface?

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

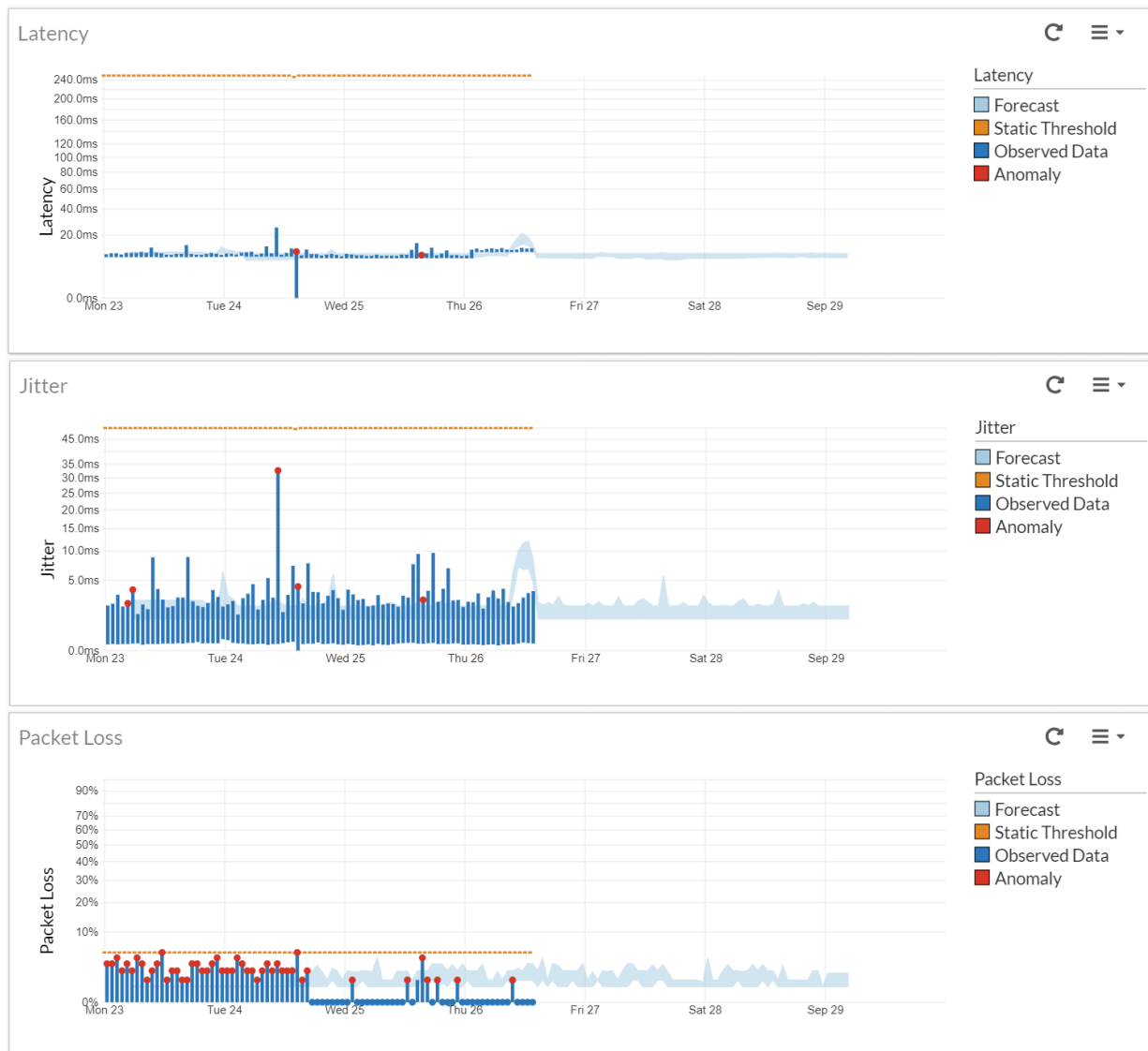
How does the predicted network performance compare to past week?

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

Health Check Trends

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

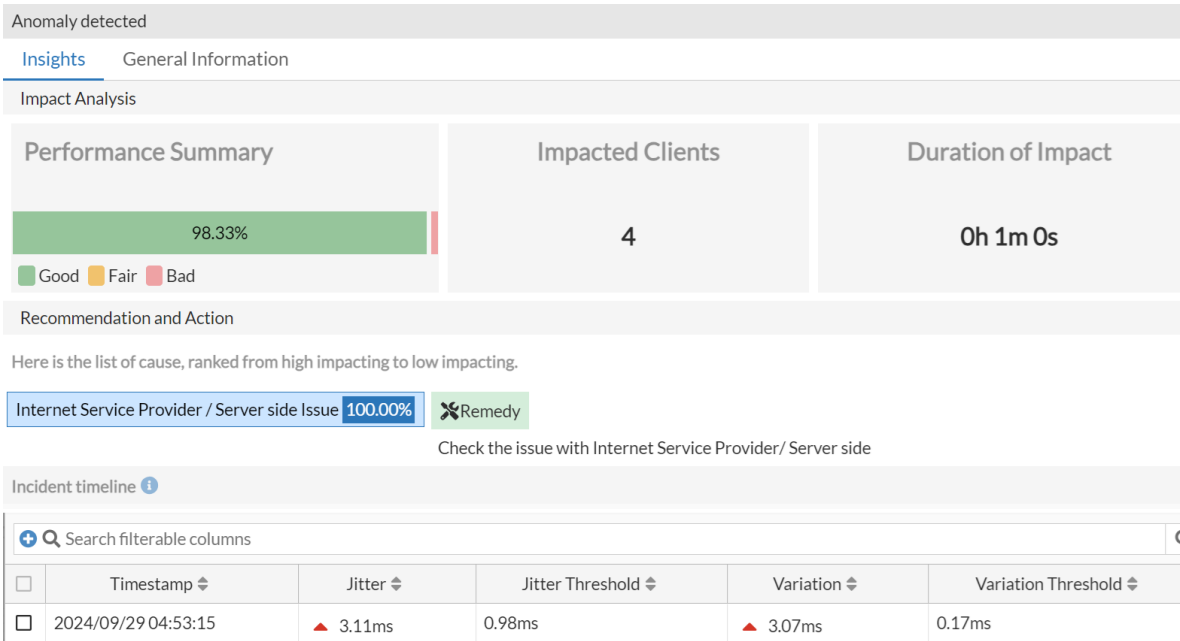
Note: The trends displayed are on an hourly basis.



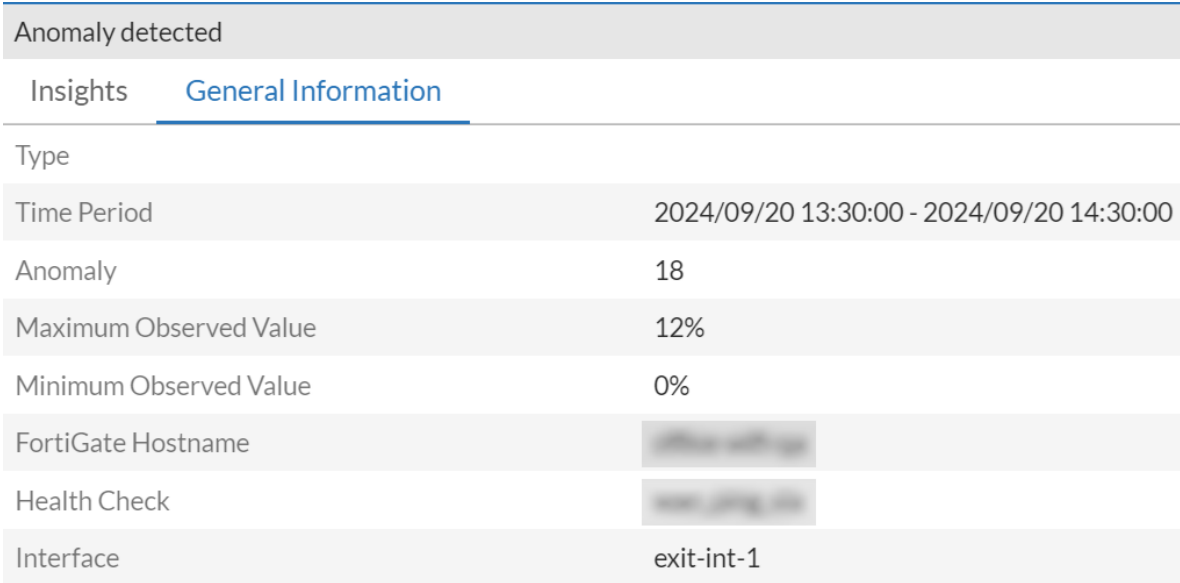
- **Forecast** - This is indicative of the range predicted by FortiAI Ops based on historical statistics.
- **Observed Data** - This is the range of real time statistics observed in a given hour.
- **Anomaly** - Anomalies are reported when FortiAI Ops observes a deviation in the data exceeding the usual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

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

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

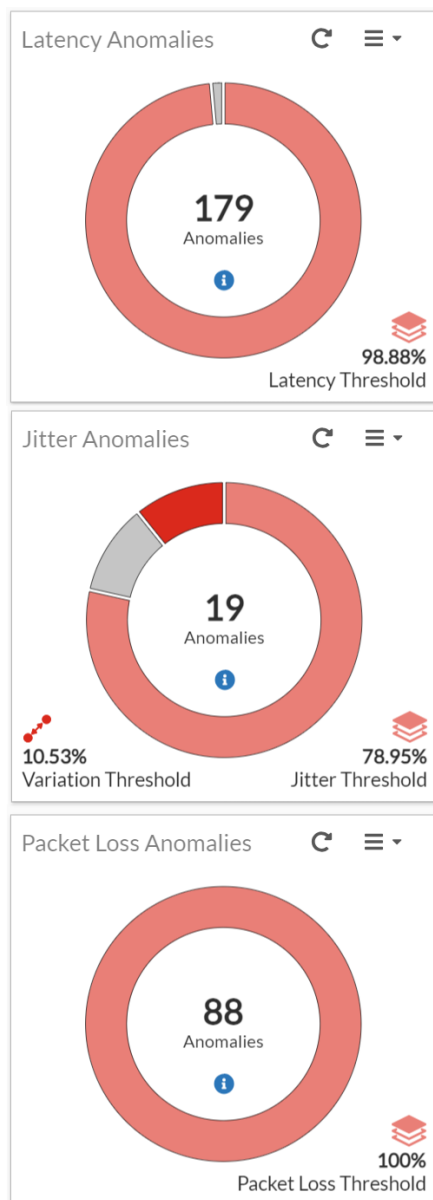


- **General Information** - This provides general information about the detected anomaly such as, the duration, the FortiGate host name, interface, configured health check, and so on.



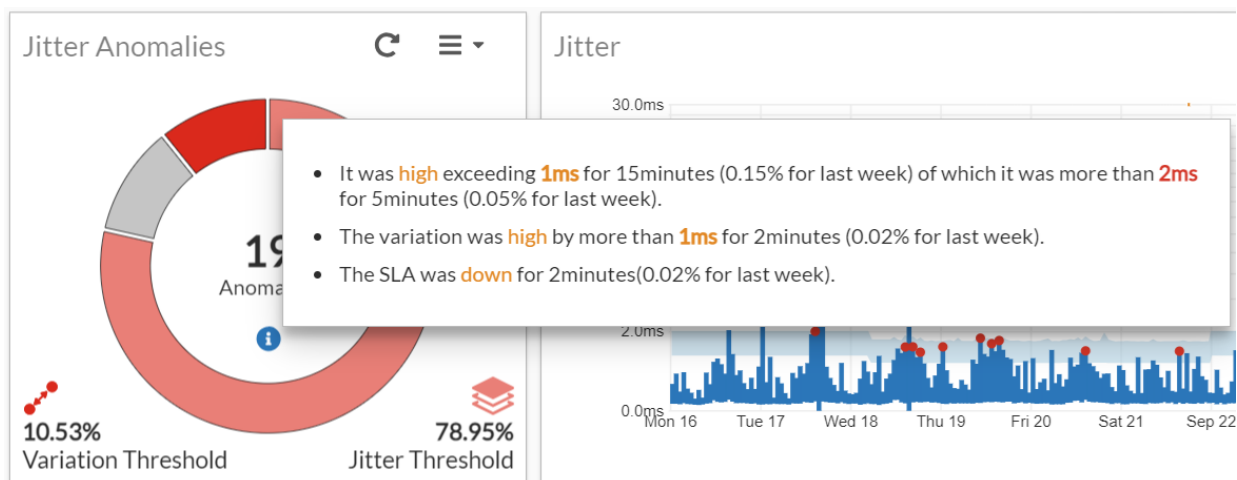
Anomalies

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



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

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



Security Fabric

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

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

- [Physical Topology](#)
- [Logical Topology](#)

Physical Topology

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

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

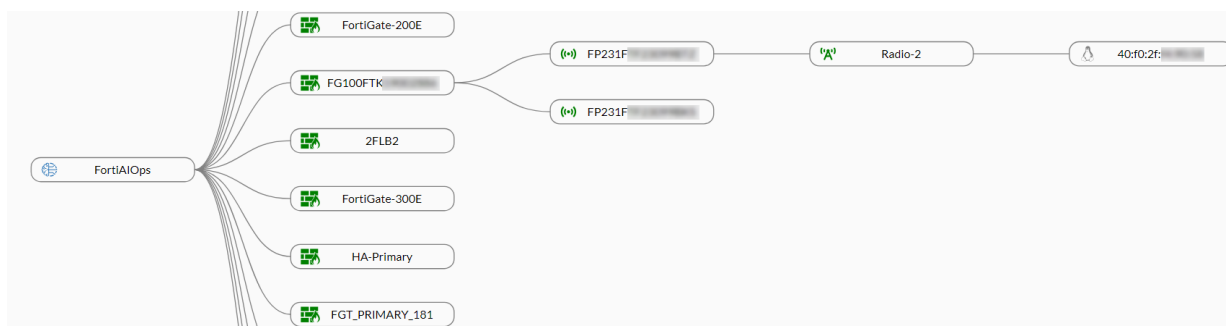
Physical Topology Filters		✕
Select Devices	2FLB2	✕
	+	
Select APs	PS223E: [REDACTED]	✕
	PS423E: [REDACTED]	✕
	+	
Select OS	Android12	✕
	Windows	✕
	+	

Show online devices ☒

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

Access Points : FP321E!	FP431FTF200...	Devices : 2FLB2, HA-Primary	OS : Android12, Windows	Online devices : Yes
-------------------------	----------------	-----------------------------	-------------------------	----------------------

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



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

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

Logical Topology

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

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

Logical Topology Filters

Select ESS

210-2Tunnel

210-43X

+

Select VLANs

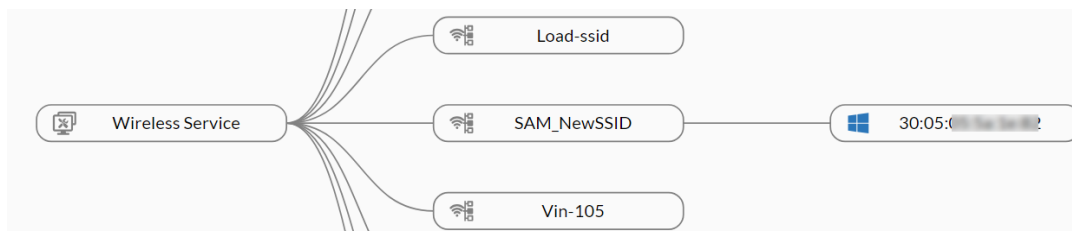
+

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

ESS : Load-ssid

VLANs : All

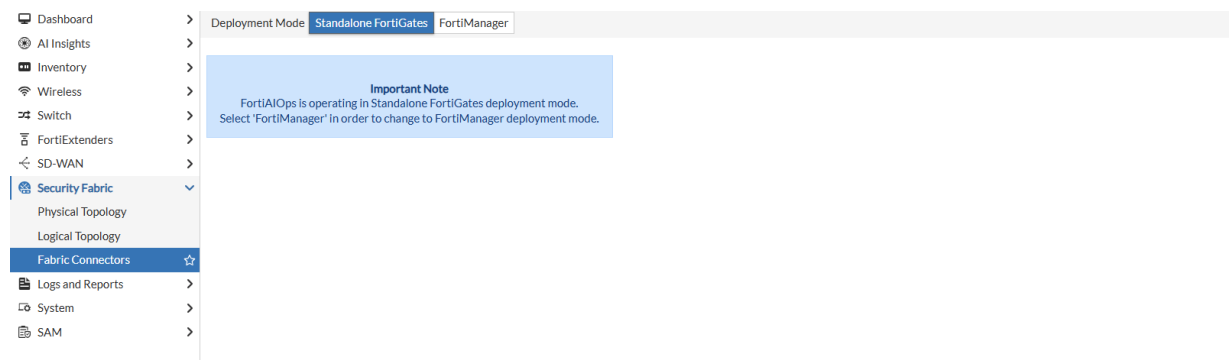
The collapsible/expandable hierarchy of entities in the logical topology is wireless service ~ **ESS** ~ **VLAN** ~ **client**; each of the entities displayed is click-able to display the next level of hierarchy.



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

Fabric Connectors

The **Fabric Connectors** window enables you to manage the **Deployment Mode**. This setting determines how FortiAI Ops discovers and communicates with network devices.



The following two deployment modes are displayed:

Standalone FortiGates

In this mode, FortiAI Ops operates independently and establishes direct connections to individual FortiGate devices.

Note: This is the default mode.

FortiManager

A centralized mode where FortiAI Ops connects via the FortiManager Fabric Connector instead of communicating with devices individually.

Note: This mode requires FortiManager version 7.6.7 or 8.0.0, which will be released at a later date.

Logs and Reports

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

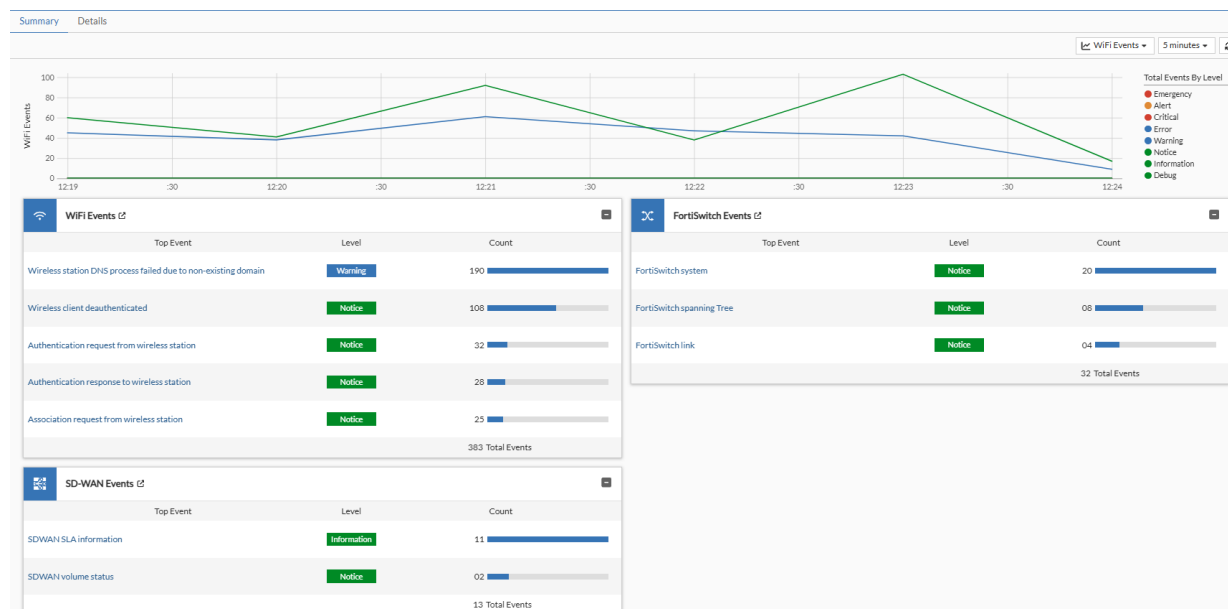
- [Event Logs](#)
- [Local Logs](#)
- [Reports](#)

Event Logs

The FortiAIOps provides a robust logging environment that enables you to monitor, store, and report WiFi events, FortiSwitch events, and SD-WAN events. The **Summary** tab displays the top five most frequent events in each type of event log along with the severity level and the total count. A line chart displays aggregated events by each severity level. Clicking on a peak in the line chart displays the specific event count for the selected severity level.

The following event logs are available:

- [WiFi Events](#)
- [FortiSwitch Events](#)
- [SD-WAN Events](#)



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

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

WiFi Events

Summary Details											
Log Description == Wireless station DNS process failed due ... X Q Search											
	Date/Time	Level	Action	Message	SSID	Station MAC	Log ID	FortiGate Serial Number	Hostname	FortiAP	Relative Date/Time
☐	2025/06/12 12:50:38	■ ■ ■ ■ ■ ■ ■ ■	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from client 18:1b:1b failed with non-existing domain	Forti-C	18:1b:1b	0104043673	FG3H	381	office	FP8: 22 seconds ago
☐	2025/06/12 12:50:37	■ ■ ■ ■ ■ ■ ■ ■	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from client 08:1b:1b failed with non-existing domain	Forti-C	08:1b:1b	0104043673	FG3H	381	office	FP8: 24 seconds ago
☐	2025/06/12 12:50:36	■ ■ ■ ■ ■ ■ ■ ■	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from client 44:1b:1b failed with non-existing domain	Forti-C	44:1b:1b	0104043673	FG3H	381	office	FP8: 25 seconds ago
☐	2025/06/12 12:50:36	■ ■ ■ ■ ■ ■ ■ ■	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from client 44:1b:1b failed with non-existing domain	Forti-C	44:1b:1b	0104043673	FG3H	381	office	FP8: 25 seconds ago
☐	2025/06/12 12:50:33	■ ■ ■ ■ ■ ■ ■ ■	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from client 08:1b:1b failed with non-existing domain	Forti-C	08:1b:1b	0104043673	FG3H	381	office	FP8: 28 seconds ago
☐	2025/06/12 12:50:33	■ ■ ■ ■ ■ ■ ■ ■	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from client 08:1b:1b failed with non-existing domain	Forti-C	08:1b:1b	0104043673	FG3H	381	office	FP8: 28 seconds ago

The following log details are displayed for each event.

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

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

Log Details

General

Absolute Date/Time

2025/06/12 14:56:35

Time

14:56:36

Virtual Domain

root

Log Description

Wireless client deauthenticated

Source

MAC Address

3e:71:00:00:00:c8

Interface

2

SSID

Forti-C[REDACTED]F

User

N/A

Action

Action

deauth

Reason

Reserved 0

Security

Level

Security Mode

WPA2 Enterprise

Encryption

AES

Cellular

Serial Number

FP831FTF21000244

Event

Physical AP

FP8[REDACTED]244

Message

AP sent deauthentication frame to client

3e:72:00:00:00:08

Other

Log event original timestamp

1747920395809895450

Timezone

+0530

Log ID

0104043575

Type

event

Sub Type

wireless

Close

FortiSwitch Events

Summary		Details	
Log Description == FortiSwitch system x 0 Search filterable columns			
	Date/Time	Level	Message
☐	2023/06/12 14:10:15	ERROR	error:0A000126:SSL routines:unexpected eof while reading --
☐	2023/06/12 14:09:51	ERROR	error:0A000126:SSL routines:unexpected eof while reading --
☐	2023/06/12 14:09:41	ERROR	The ntp server 208.91.112.60 is determined unreachable at Thu Jun 12 14:09:41 2023
☐	2023/06/12 14:09:29	ERROR	error:0A000126:SSL routines:unexpected eof while reading --
☐	2023/06/12 14:09:23	ERROR	error:0A000126:SSL routines:unexpected eof while reading --

The following log details are displayed for each event.

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

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

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

Log Details	
General	
Absolute Date/Time	2025/06/12 14:53:41
Time	14:53:41
Virtual Domain	root
Log Description	FortiSwitch system
Source	
User	Fortilink
Message	
Message	The ntp server 201.10.10.10.2.62 is determined unreachable at Thu Jun 12 14:53:41 2025
Security	
Level	
Cellular	
Serial Number	S248DF3X16000551
Other	
Log event original timestamp	1749720221204851006
Timezone	+0530
Log ID	0115032699
Type	event
Sub Type	switch-controller
User Interface	N/A
Name	S248DF3X16000551

SD-WAN Events

Summary											Details					
Log Description == SD-WAN SLA information												Search filterable columns		SD-WAN Events	5 minutes	
	Date/Time	Level	Log Description	Message	Log ID	FortiGate Serial Number	Hostname	Interface	Health Check	VDOM						
☐	2025/04/12 14:36:33	Information	SD-WAN SLA information	Health Check SLA status.	0113022925	FG310B01	office-01	exit-1	wan_ping_sla	root						
☐	2025/04/12 14:36:31	Information	SD-WAN SLA information	Health Check SLA status.	0113022925	FG310B01	office-01	exit-1	wan_ping_sla	root						
☐	2025/04/12 14:35:33	Information	SD-WAN SLA information	Health Check SLA status.	0113022925	FG310B01	office-01	exit-1	wan_ping_sla	root						
☐	2025/04/12 14:35:31	Information	SD-WAN SLA information	Health Check SLA status.	0113022925	FG310B01	office-01	exit-1	wan_ping_sla	root						

The following log details are displayed for each event.

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

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

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

Log Details

General

Absolute Date/Time

2025/06/12 14:36:33

Time

14:36:34

Virtual Domain

root

Log Description

SDWAN SLA information

Source

Interface

exit-i

Health Check

wan_ping_sla

Message

Message

Health Check SLA status.

Security

Level

Other

Log event original timestamp

1749719193775663143

Timezone

+0530

Log ID

0113022925

Type

event

Sub Type

sdwan

Jitter

0.495

Latency

6.874

Packet Loss

0.000

MOS Value

4.400

MOS Coder

g711

Used Upstream

1.07Mbps

Available Upstream

0kbps

Used Downstream

5.45Mbps

Available Downstream

0kbps

Used Bandwidth

6.52Mbps

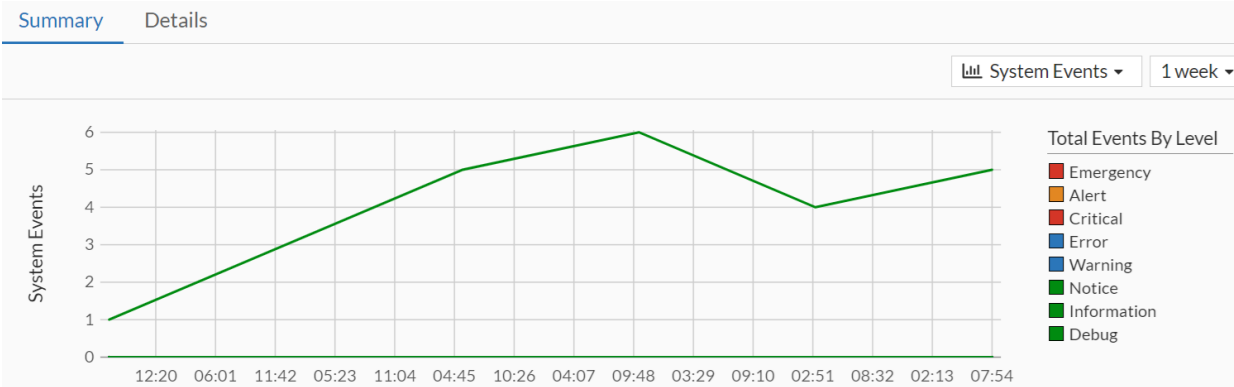
Available Bandwidth

0kbps

Close

Local Logs

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



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

Summary Details					
+ Q Search filterable columns					
Q System Events Details 1 week					
	Date/Time	Level	Message	Log Description	Log ID
☐	2024/09/28 18:07:20	Notice	Diagnostics file for fortiaioops created successfully.	Diagnostics and Tools	0006018001
☐	2024/09/28 18:07:20	Notice	Diagnostics file for application created successfully.	Diagnostics and Tools	0006018001
☐	2024/09/28 18:07:20	Notice	Diagnostics file for system created successfully.	Diagnostics and Tools	0006018001

Reports

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

- [Creating Reports](#)
- [Viewing Reports](#)
- [Scheduled Reports](#)
- [PCI Reports](#)

Creating Reports

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

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

Basic Information

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

BASIC INFORMATION

Category

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

Report Type

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

[Sample Reports](#)

Name

Report Template [0-256] chars.

Report Title

FortiAIOPs [0-256] chars.

Rogue MAC
[Select](#)

The following categories of reports are supported.

- [Station Reports](#)
- [AP Reports](#)
- [Inventory Reports](#)
- [Service Reports](#)
- [Application Visibility Reports](#)

Station Reports

The following types of station reports are supported.

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

Category	Description
Station Session Details	Provides the average station session trend details. A graphical summary of the station session trend details of throughput, loss, airtime utilization and noise for a connected station is displayed. The following details are displayed. - Graphs - The three types of <i>Station Session Details</i> graphs are displayed as follows. <i>Trend On Throughput</i> - This graph displays the trend of Throughput for the selected station. <i>Trend On Loss</i> - This graph displays the trend of Loss for the selected station. <i>Trend On Airtime Utilization</i> - This graph displays the trend of Airtime Utilization for the selected station. - Station Session Details - This section provides each station's Date/Time, IP4 Address, IP6 Address, Controller, AP ID, SSID, User, Throughput (Kbps), Loss%, Airtime Utilization% and AP Name.
Top Stations	The <i>Top Stations</i> report type generates reports for the busiest stations based on the <i>Throughput</i> 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 <i>Unique Station</i> 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. <i>Finger Print OS Distribution</i> - This graph displays the station distribution based on the OS Type. <i>Finger Print Device Distribution</i> - This graph displays the station distribution based on the Device Type. <i>OUI Distribution</i> - This graph displays the station distribution based on the OUI. <i>Station Distribution</i> - This graph displays the station distribution based on the RF Type. - Unique Station Details - This section provides the station's OUI, Date/Time (CST), Station MAC, User, IPv4 Address, IPv6 Address, RF Type, SSID, Device Type, OS Type and Floor.
EAP-AKA Error	The EAP-AKA Error type generates a report with details of EAP-AKA errors associated with specific ESSIDs and on specific stations connected to network within the reporting interval. The following details are displayed.

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

AP Reports

The following types of AP reports are supported.

Category	Description
Rogue Details	The <i>Rogue Details</i> 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. <i>Rogue Trend By Type</i> - The two types of <i>Rogue Trend By Type</i> graphs are displayed as follows. <i>Trend on Rogue Station</i> - This graph displays the trend type based on the number of rogue Stations. <i>Trend On Rogue AP</i> - This graph displays the trend type based on the number of rogue APs. <i>Rogue Trend By Controllers</i> - This graph displays the top 10 controllers with the highest number of rogues. - New Rogues Detected During Reporting Interval - This section provides the details of the new rogues detected during reporting

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

Inventory Reports

The following types of inventory reports are supported.

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

Service Reports

The following types of service reports are supported.

Category	Description
Service Usage Summary	Provides the service usage summary based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed. - Graph - The graphs are of the following types. <i>Top SSIDs Based on Throughput</i> - This graph displays the top SSIDs based on the throughput. <i>Top SSIDs Based on Number Stations</i> - 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 FortiAI Ops.
- **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.

RECURRENT

☐ One Time

☒ Schedule

Time

12 AM

▼

☐ Daily

☒ Weekly

☐ Monthly

Every

Monday

▼

Every

Day of Month [2-28]

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

Report Generation Options

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

REPORT GENERATION OPTIONS

File Format

☒ HTML ☐ PDF ☐ CSV

Email To:

test@fortinet.com

Customize

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

Viewing Reports

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

REFRESH DELETE							
☐	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**.

REFRESH ADD EDIT DELETE					
☐	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](#)
- [Upgrade](#)
- [Licensing](#)
- [FortiGuard](#)
- [Location Services](#)
- [Network Interface](#)
- [Certificates](#)

User Management

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

- [Users](#)
- [User Groups](#)

Users

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

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

Note:

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

User permissions are indirectly assigned through their membership in user groups. By default, all users are members of the *Default* user group. The *admin* user and all ADOMs 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 ADOM and users to the user group upon its creation to ensure that users have access to the assigned ADOM. 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.

+ Add	Edit	Delete	Search filterable columns		Q	Reload
Username	Role	Full name	Authentication Type	Server Name		
☒ admin	System Administrator	admin	LOCAL	Local Server		

- [Adding a New User](#)
- [Editing User Information](#)
- [Deleting User Information](#)

Adding a New User

Perform the following steps to add a new user:

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

User Role	Access Level
Guest	Read only access to all features in the system except system settings.
Standard_User	Read/Write privilege to all configurations and features except system settings
Super_User/ System Administrator	Read/Write access across system. All super users will have access to all ADOMs, all devices, all system settings.

7. Click **Save**.

Notes:

- Once you have created users in FortiAIOPS, it is necessary to refresh the FortiAIOPS application portal in order for the users list to be updated and displayed in the **User Groups** page.
- The super user or system administrator can provide ADOM access to a user by choosing the ADOM and the users in the user group option in FortiAIOPS application portal. See [User Groups](#).
- Users created in GUI will be synced to CLI and vice versa.
- By default, user created in CLI will have super-user access, and can be changed from GUI.

Editing User Information

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

Deleting User Information

To delete a user, select the user and click **Delete**. This action will remove the user from both the GUI and CLI.

User Groups

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

+ Add Edit Delete + Q Search			
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 ADOM that the users should be part of.
5. Select the Users from the list to be added.
6. Click **Create**.

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

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

User Sessions

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

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

User	Client IP Address	Authentication Server	Login Time	Connected Duration	User Agent	User Role
☒ admin	10.32.1.105	LOCAL	2025/04/25 07:15:55	3h 9m	Chrome	System Administrator
☐ [redacted]	10.32.1.105	LOCAL	2025/04/25 07:19:55	3h 5m	Chrome	Super_User
☐ [redacted]	10.32.1.105	LOCAL	2025/04/25 07:36:34	2h 48m	Chrome	Super_User
☐ [redacted]	10.32.1.105	LOCAL	2025/04/25 08:04:47	2h 20m	Chrome	Super_User
☐ admin	10.32.1.105	LOCAL	2025/04/25 09:26:20	58m 36s	Chrome	System Administrator
☐ admin	10.32.1.105	LOCAL	2025/04/25 10:23:44	1m 12s	Chrome	System Administrator

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

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

Users Sessions limit

Number of active Sessions *

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

Note:

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

Backup and Restore

The **Backup and Restore** page provides valuable tools for managing and maintaining backups of the FortiAI Ops configuration. This page includes options for taking, uploading, restoring, downloading, and deleting backups.

Note: This release supports the backup and restore function only for FortiAI Ops configuration. CLI configurations are saved using the `execute backup config` command and it does not include any FortiAI Ops specific configurations.

File Name	Status	Timestamp	File Size
Backup-fortiaioops_v2.0.0-build0031-admin-2023-04-04-01-05-01.tar	Available	2023/04/04 06:35	50.7M

Take Backup

The **Take Backup** function allows you to take a backup of the FortiAIOps configuration. This information can be saved as a file (.tar) and used to restore the configuration and settings at a later time.

To perform the backup operation, perform the following steps:

1. Navigate to **System > Backup and Restore**.
2. Click **+ Take Backup**.
3. Select **Backup Option**, as **Configuration only**. Backing up only the configuration includes information like maps, controller details, and AP details except statistics data.
4. Select the **Backup Type**. Choose between **Disable Backup**, **Backup now**, and **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 <input checked="" type="button" value="Schedule for later"/>
Backup Option	<input checked="" type="button" value="Configuration only"/>
Backup Schedule	Daily <input checked="" type="button" value="Weekly"/>
Backup Day	<input checked="" type="button" value="Sunday"/> Monday Tuesday Wednesday Thursday Friday Saturday
Backup Hour	5 PM
Number of backups to preserve	1 2 <input checked="" type="button" value="3"/>

Upload

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

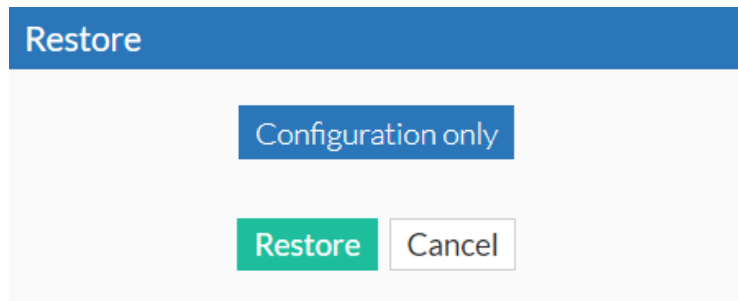
1. Navigate to **System > Backup and Restore**.
2. Click **Upload**.
3. Browse and select the backup file (.tar) file.
4. Click **Upload**.

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](#)
- [Administration Settings](#)
- [OUI Update](#)
- [General Logs](#)
- [Mail Server](#)
- [Authentication Servers](#)

Network Settings

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

Network Settings

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

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

Edit Hostname

Hostname	app
----------	----------------------------------

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

Edit System Time

Current System Time

2023/10/13 16:05

Time Zone

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

Time Setting method

Synchronize with NTP Server

Set Server(s)

1

pool.ntp.org

2

ntp2.fortiguard.com

remove

Add more servers

Notes:

- Both FortiAIOPs and FortiGate must be synchronized with an NTP server.
- Reboot the system (execute `reboot` command) after the NTP and timezone settings are configured.

Statistics

This section allows you to configure data retention period in FortiAIOPs. All monitoring data is stored based on dynamically allocated or manually configured duration.

- Auto config duration to keep Statistics data** - This feature allows FortiAIOPs to dynamically configure the statistics retention period based on daily data accumulation and the available space for maximum data storage. This is enabled by default for a period of 3 weeks, but based on daily monitoring of the data accumulation and available space, FortiAIOPs automatically adjusts the statistics retention period.
- Duration to keep statistics data** - Manually configure the weeks or months to retain and preserve the statistics data. The permissible range is 1 to 3 weeks or 1 to 6 months. The statistics data older than the time period specified in this field from the current date, is automatically deleted from the FortiAIOPs server. If the duration configured here requires more than the available space for statistics retention, then FortiAIOPs throws an error.

Statistics

Auto config duration to keep Statistics data

i

Duration To Keep Statistics Data

2 weeks ▾

Notes:

- You are allowed to configuring the statistics retention duration manually only based on the available disk space.
- The AI Insight statistics are stored for a maximum period of 1 week.
- Post-upgrade, the configured **Duration to Keep Statistics Data** is retained with **Auto config duration to keep Statistics data** enabled. Based on daily analysis, FortiAIOPs configures the statistics retention period automatically.

Administration Settings

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

 Administration Settings

Certificate

default ▼

Apply Certificate

OUI Update

This section allows you to view and manage the OUI details.

- **Last update time** - Displays the date and time of the OUI details updated the last time.
- **Parsing status** - Displays the status of parsing.
- **Automatically update every week** - This option when enabled, will allow the system to automatically update the OUI details every week.
- **Upload OUI File** - To upload OUI file, click **Choose File**, browse and select the OUI file, and click **Upload**.

 OUI Update

Last update time

Parsing status

Automatically update every week

Upload OUI File

completed



Choose File

No file chosen

Upload

General Logs

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

 General Logs

Syslog logging

IP address / FQDN

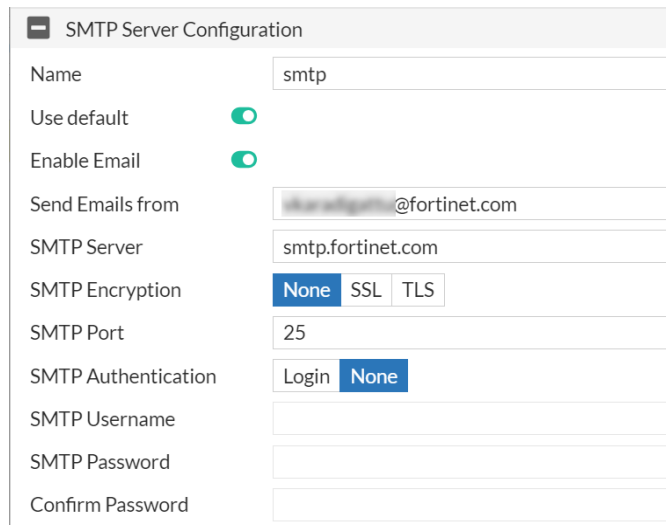


10.1.1.1

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

Mail Server

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



SMTP Server Configuration

Name: smtp

Use default: ☒

Enable Email: ☒

Send Emails from: [redacted]@fortinet.com

SMTP Server: smtp.fortinet.com

SMTP Encryption: **None** | SSL | TLS

SMTP Port: 25

SMTP Authentication: Login | **None**

SMTP Username:

SMTP Password:

Confirm Password:

Configure the following SMTP server settings.

- **Use default** - If enabled, the current configurations are used as the default for all SMTP server communication.
- **Send Emails from** - Enter the email address to trigger the email notifications from.
- **SMTP Server** - Enter the IP address or the hostname of the SMTP server.
- **SMTP Encryption** - Select the security mode as **SSL** or **TLS**. Select **None** to not use any encryption.
- **SMTP Port** - Enter the port number used to connect to the SMTP server.
- **SMTP Authentication** - Select the authentication via **Login** and enter the **SMTP Username** and **SMTP Password**. Select **None** to not use any authentication for the SMTP server.

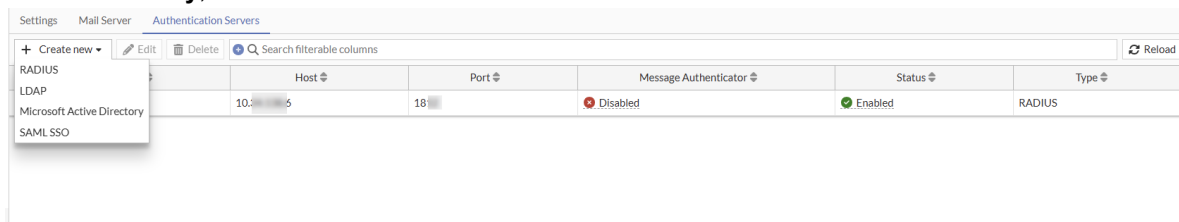
Authentication Servers

Remote users can be authenticated using remote servers.

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

To add an Authentication Server:

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



Settings Mail Server Authentication Servers						
+ Create new Edit Delete Search filterable columns Reload						
	Host	Port	Message Authenticator	Status	Type	
	10.3.1.5	18	Disabled	Enabled	RADIUS	

3. Configure the following settings for the server to be added:

- **LDAP Server:**

LDAP Authentication Server X

Name *	LDAP_WIN19
Host *	10. .6
Port *	
Protocol Agent *	Windows LDAP ▾
Encryption *	NONE ▾
Base DN *	DC= ,DC=local
Anonymous Admin Allowed *	☒
Admin Bind DN *	CN= ,DC=local
Update Password	☒
Admin Password	••••••••
Confirm Password *	••••••••

Name	Enter a name to identify the LDAP server.
Host	Enter the IP address of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Protocol Agent	Select the LDAP server type (LDAP or Windows Active Directory) to ensure correct authentication and directory attribute handling.
Encryption	Select encryption from the drop-down. Choose between NONE and LDAPS.
Base DN	Enter the base Distinguished Name (DN) for the LDAP server. This specific entry in the directory hierarchy acts as the starting point for the search operations in the LDAP server.
Anonymous Admin Allowed	Enable to allow anonymous admin user.
Admin Bind DN	Enter the Admin user Distinguished Name (DN).
Admin Password	Enter a password for admin user.
Confirm Password	Enter the password again to confirm.

- **RADIUS Server:**

RADIUS Authentication Server

Name *

Fguest_radius

Server Name/IP Address *

10.3

Port *

1812

Update Secret

☒

Server Secret

••••••••

Test Connectivity

Test User Credentials

Message Authenticator *

☒

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

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

Microsoft Active Directory ×

Name *	Microsoft AD 2012
Host *	10.3
Port *	389
Encryption *	NONE ▾
Base DN *	DC=apps DC=com
AD Domain *	AP COM
AD Admin bind Username *	pratl
Update Password	☒
Admin Password	••••••••
Confirm Password *	••••••••

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

- **SAML SSO:**

Name	A user-defined name to identify this SAML SSO configuration.
Protocol Agent	Specifies the SAML identity provider type (Generic SAML or Microsoft ADFS) to ensure proper SSO interoperability and attribute handling.
Server	The IP address or FQDN of the Identity Provider (IdP) server where SAML authentication requests will be sent.
Enabled	Toggle button to enable or disable this SAML SSO configuration. If enabled, SAML SSO is active. If disabled, configuration is saved but inactive.
Auto Create Admin	When enabled, SSO admins will be created automatically if they do not exist.
Default Admin Profile	This determines the default permissions available to the SAML-based admin user when they initially login. This can be modified after the admin's initial login. The permission is listed as Guest, Standard_user, Super_user.
Identity Provider	
Entity Id	The unique identifier URL for the Identity Provider. This is usually the IdP metadata URL. For example - http://<IP address>/saml-idp/corpalops/metadata/
Single Sign-On Service Endpoint	The URL where FortiAI Ops will redirect users for authentication (IdP SSO login URL). For example -

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

Attribute used to identify email	The name of the attribute in the SAML assertion provided by the Identity Provider (IdP) which contains the email address.
Attribute used to identify groups	The name of the attribute in the SAML assertion provided by the Identity Provider (IdP) which contains the user's group memberships.
Note: You can enter either the fixed keywords username, email and groups or specify the exact attribute names as configured in your Identity Provider.	

4. Click **Save**.

Note:

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

Upgrade

Navigate to **System > Upgrade** to upload the FortiAI Ops image file and upgrade FortiAI Ops.

Upload firmware image file



[Select file](#) .gz, .out files
or drag and drop it here

✓

—

📄

—

🔄

—

✓

Upload Image

Verify Image

Upgrade

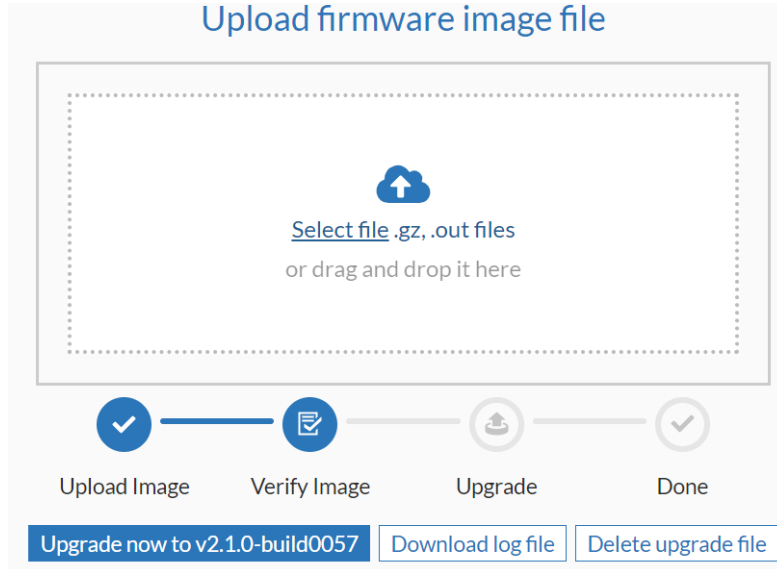
Done

Upgrade now to v2.1.0-build0057

Download log file

Delete upgrade file

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



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

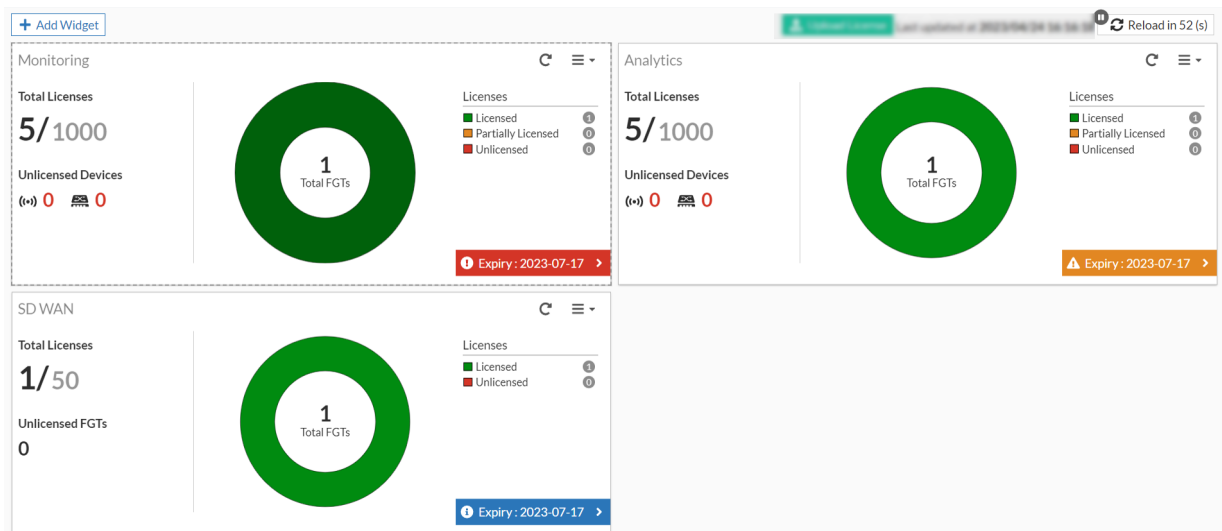
Licensing

The licensing page displays the license information including the current license status, expiration date, and the number of Monitoring, Analytics and SD-WAN licenses.

- **Monitoring** - displays the number of license consumed for monitoring and the number of switches or APs that are unlicensed. The doughnut chart shows the count of FortiGates that are licensed, partially licensed and unlicensed. Click on the filters to view license information in detail. For monitoring license, the consumption is based on the number of switches or APs added.
- **Analytics** - displays the number of license consumed for analytics and the number of switches or APs that are unlicensed. The doughnut chart shows the count of FortiGates that are licensed, partially licensed and unlicensed. Click on the filters to view license information in detail. For analytics license, the consumption is based on the number of switches or APs added.
- **SD-WAN** - displays the number of license consumed for SD-WAN and the number of FortiGates that are unlicensed. The doughnut chart shows the count of FortiGates that are licensed and unlicensed. Click on the filters to view license information in detail. For SD-WAN license, the consumption is based on the number of FortiGates added.

Notes:

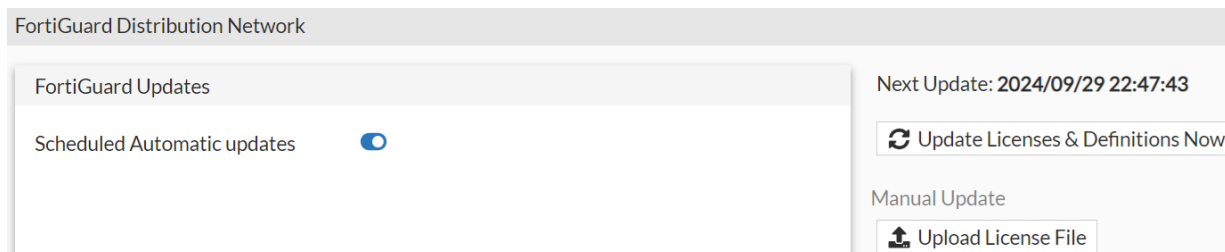
- If you buy additional licenses or extend the existing ones through FortiCare, the expiration date displayed will show the nearest expiry and will not include the newly added license. To see the accurate license details, please check FortiCare portal.
- To purchase a co-term license or add any required extra devices to current licenses, please contact your distributor or Fortinet renewal team.



FortiGuard

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

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



Location Services

The **Location Services** window displays the **Project Name** and **Secret Key** which are unique security credentials generated for FortiAI Ops to authenticate communication from your access points. These credentials allow the FortiAP to send location telemetry to FortiAI Ops.

Location Services	
Project Name	FortiAIOPS
Secret Key	8 [REDACTED] a9
Location Services Status	☒ Enabled

You must configure the FortiAIOPS authentication details in the FortiAP profile before enabling the service. Once configured, enable the **Location Service Status** toggle button.

Use the following steps to configure the details in FortiAP profile:

1. From the FortiGate GUI, navigate to **WiFi & Switch Controller > FortiAP Profiles**.
2. Select the FortiAP profile you want to configure FortiAIOPS for.
3. Navigate to **Location Based Services** section and select the **FortiPresence** mode you want to use to enable the service.

Location Based Services	
FortiPresence	
Mode	Disable Foreign Channels Only <input checked="" type="button" value="Foreign and Home Channels"/>
Project name	FortiAIOPS
Password	 Change
FortiPresence server type	<input checked="" type="button" value="IP"/> FQDN
FortiPresence server IP 	10.34.152.160
FortiPresence server port	4013
Report rogue APs	☒
Report unassociated clients	☒
Report transmit frequency (in seconds)	5
☐ Ekahau blink	
☐ AeroScout	
Locate WiFi clients when not connected ☒	

4. Enter the **Project name** and **Password** from FortiAIOPS (Use the **Project Name** and **Secret Key** from the **FortiAIOPS GUI System > Location Services**).
5. Enter the **FortiPresence server IP** as FortiAIOPS IP address.
6. Enter the **FortiPresence server port** as 4013.
7. Enable **Report rogue APs** toggle button (If you want the Rogue AP location feeds to be reported in FortiAIOPS).
8. Configure the **Report transmit frequency (in seconds)** (Recommended: 30 seconds).
9. Click **OK** and save the FortiAP Profile.

Note: that a minimum of 3 APs must be placed on the map for the locating service to detect them.

For information on the FortiGate configuration, see the [Configuration Guide](#).

Network Interface

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

Edit Interface

Name

port1

Mode

DHCPStatic

IP Address

10.34.10.1

Netmask

255.255.255.0

Type

LogicalPhysical

AllowAccess

☒ HTTP

☒ HTTPS

☒ PING

☒ SNMP

☒ SSH

☒ TELNET

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

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

Click **Update**.

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

Create Route

Device	port2 ▼
Destination	10.1.1.1
Gateway	10.2.1.1

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

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

Interfaces	Static Routes	DNS
------------	---------------	------------

Primry DNS Server	208.91.134.100
Secondary DNS Server	208.91.134.101

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.

The Local Certificates section also enables you to import a certificate. The supported formats are .cer, .crt, .tar, .tar.gz, tgz, zip, tar.xz, and .xz.

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

Reset

Generate

Cancel

CA Certificates

The CA Certificates section allows you to install and manage your CA certificate. To install a CA certificate, click **Install CA Certificate** and upload your CA certificate (.pem or .cer file). You can view details, download, or delete selected CA certificate after installation.

Notes:

- To upload certificates, the Root CA, server certificate, and key file must be bundled together and uploaded in any of the supported formats.
- Certificates can only be uploaded in PEM or CER formats. Other formats are not supported. If the certificate is in any other format, such as P12 or PFX, it must be converted to a supported format before uploading.
- When using CA2, the intermediate and root CA content must be combined into a single text file (.pem file). This is necessary because only three files can be included in the bundle uploaded: Root CA, server certificate, and key file.
- To access FortiAIOps using a custom domain name, you must install the required CA and Server certificates for the domain configured on FortiAIOps.

SAM

Service Assurance Manager (SAM) is a predictive diagnostic software with trouble-prevention capability. It diagnosis the health of the wireless network and reports the issue before the users are impacted. The FortiAIOPS infrastructure is used to perform on-demand end-to-end system tests. The SAM mode is activated in FortiAP during SAM tests. In this mode, FortiAP radios operate as a client and perform tests against another AP. Once baseline network performance is established, any schedule tests that deviate from the baseline/threshold are marked based on the SAM test values. Multiple tests can be configured with SAM.

- Connectivity tests to measure packet loss
- Throughput tests to measure performance

The tests can be configured to run on a WPA2 PSK SSIDs available in the FortiGate. SSIDs can only be configured in FortiGate.

Notes:

- The SAM is supported only for the following.
 - F-series, G-series, and K-series FortiAPs. Currently only radio 1 (2.4GHz) and radio 2 (5GHz) are supported for SAM operations.
 - Bridge mode SSIDs
 - WPA2 PSK security mode
 - Radios in AP mode.
- SAM tests are not supported on radio 3 of the K-series and G-series FortiAP models.
- While running SAM tests, FortiAIOPS modifies the FortiAP Profile that is configured on the Access Point in FortiGate. As a result, the CAPWAP on the FortiAP is restarted.
- Creating a SAM test causes the following changes to your WLAN network, and these changes impact the clients connected to the FortiAP.
 - New FortiAP profiles are created to run the SAM tests.
 - Schedule and baseline tests are run immediately.
- [Trends](#)
- [Completed Tests](#)
- [Baseline Tests](#)
- [Schedule Tests](#)

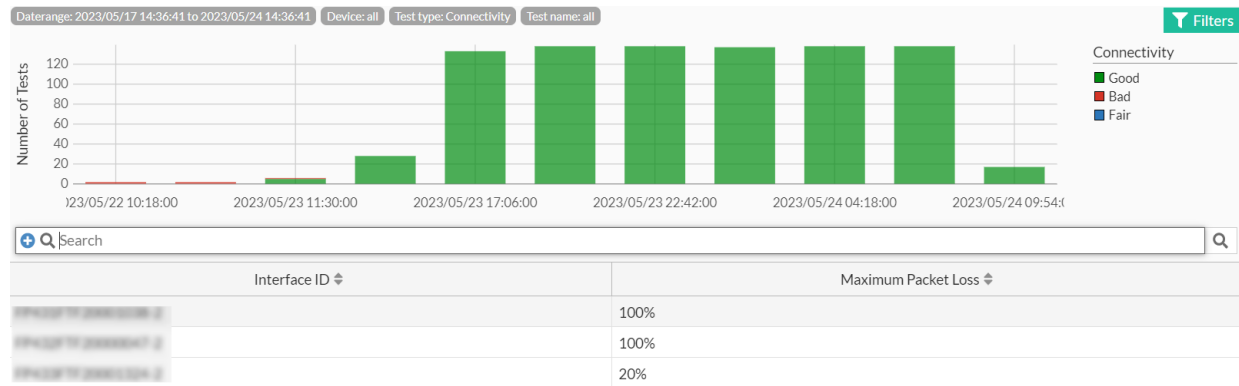
Trends

The Trends page in the Service Assurance section of FortiAIOPS provides a comprehensive overview of network test performance. You can analyze the total number of tests performed, their categorization as Good, Fair, or Bad, and gain insights into interface-specific data such as Interface IDs and Maximum Packet Loss values.

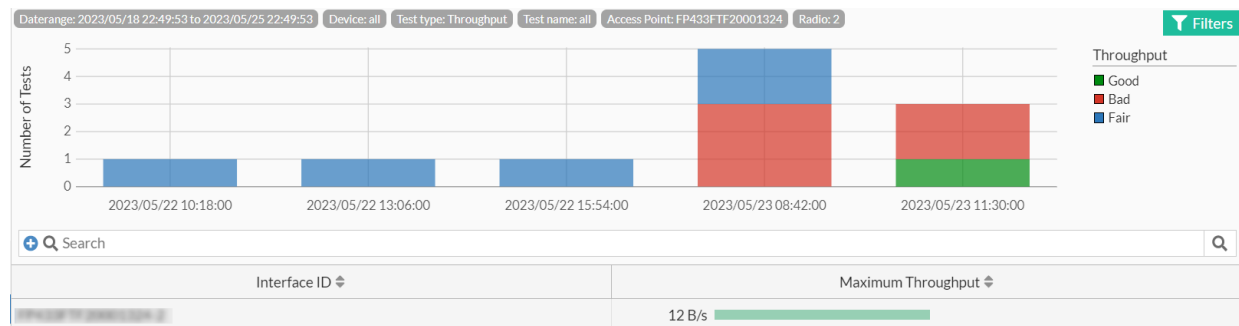
The bar chart classifies the total number of tests performed into three categories: *Good*, *Fair*, and *Bad*. This classification allows you to quickly assess the overall performance of the network based on the test results.

Each bar represents a specific time period, enabling you to identify trends and patterns in test performance over time.

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



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



To filter the results in the bar chart, click the desired Interface ID.

Trend Filters

The Trends page offers various filters to refine the displayed data and narrow down the analysis. The available filters include:

- **Select Device** - Select a specific device from the available options to filter the test results associated with that device.
- **Test Type** - Choose between the *Connectivity* or *Throughput* test types to filter the relevant test results.
- **Test Name** - Select a specific test name to filter the test results associated with that particular test.
- **Start Date and End Date** - Specify a start date and end date to filter the test results within a specific time range.

Trend Filters

Select Device

Test Type Connectivity Throughput

Test Name

Start date

End date

Completed Tests

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

Completed Tests

Completed Tests					
Delete Search					
Name	SSID	Test Type	Device Name	End Time	Result
Sch_thput	sam...ut	Throughput	PC1_PRIMARY_S01	2023/05/20 16:05:20	0 1 0 0
Sch_thput_TCP	sam...qa	Throughput	PC1_PRIMARY_S01	2023/05/20 16:23:37	0 1 0 0
Sch_conn_instant	sam...wpa	Connectivity	PC1_PRIMARY_S01	2023/05/20 16:27:56	0 1 0 0
Sch_conn_cont	sam...ut	Connectivity	PC1_PRIMARY_S01	2023/05/20 16:37:06	1 0 0 0

Best Fit Columns
Reset Table
Select Columns

☒ Name
☒ SSID
☒ Test Type
☒ Device Name
☒ End Time
☒ Result
☐ Bad Results
☐ Device IP Address
☐ Device Serial
☐ Fair Results
☐ Good Results
☐ Start Time
☐ Unknown Results

Apply Cancel

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 X Status == good X Start Time = 2023-05-24 12:39:40 X + Q Search							
Test name	Test Type	AP name	SSID	Radio ID	Band	FortiGate Name	Serial Number
Sch_conn_101F	Connectivity	(*)	sa	1	2.4GHz		

- **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					
+ Q Search					
Name	SSID	Test Type	Sweep Mode	Device Name	State
test_conn_binary	sam	Connectivity	recurring	test	Waiting
sch_cont_VenkatFGT	sam wpa	Connectivity	recurring	test	Running
Throuput_cont	sam out	Throughput	recurring	test	Running
Sch_HA_conn	sam	Connectivity	recurring	test	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 Tests

Baselines serve as reference points for evaluating the health and performance of the wireless network. Baselines play an important role in detecting deviations from expected network behavior. SAM allows for the configuration of multiple tests, including connectivity tests to measure packet loss and throughput tests to assess overall performance.

View details + Q Search							
Name	Test Type	Baseline Type	Device Name	Device Serial	Device IP Address	Status	Start Time
Base_24	Connectivity	Measured	test	test	test	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 **SAM > Baseline**.
2. Click **+ Add**.
3. Provide the following details:

Add baseline test ×

Details

Name

Connectivity_baseline

Test Type

Connectivity Throughput

Device

office- ▼

AP Radios

1.8: 1 ×

+

Baseline Type

Configured Measured

SSID

SSID-1

Pre-shared Key

••••••••

Ping Server

1.1.1.1

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

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

Are you sure you want to proceed?

Add

Cancel

- **Name:** Name for the baseline.
- **Test Type:** Select **Connectivity** as Test Type to measure packet loss.
- **Device:** Select the device.

- **AP Radios:** Select AP radios.
- **Baseline Type:** Select baseline type, **Configured** or **Measured**
- **SSID:** Enter SSID name. SSID must be configured on a neighboring AP in FortiGate.
- **Pre-shared Key:** Enter the pre-shared key for the SSID.
- **Packet Loss(%):** Enter packet loss value in %.
Note: Packet Loss(%) field is displayed only when **Configured** is selected as baseline type.
- **Ping Server:** Enter **IP address** or **FQDN** of the ping server to perform connectivity tests.

4. Click **Add**.

Throughput Baseline

To create a throughput baseline, perform the following steps:

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

Add baseline test

Details

Name

Throughput_baseline

Test Type

Connectivity
Throughput

Device

office-

AP Radios

1.81

Baseline Type

Configured
Measured

SSID

SSID-1

Pre-shared Key

••••••••

Protocol

TCP
UDP

iPerf Server

10.1

Port

8001

Important Note:

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

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

Add

Cancel

- Name: Name for the baseline.
- Test Type: Select **Throughput** as test type to measure performance.
Note: Ensure that the network should have Iperf server running iperf3 traffic.

- Device: Select the device.
- AP Radios: Select AP radios.
- Baseline Type: Select baseline type, **Configured** or **Measured**.
- SSID: Enter SSID name. SSID must be configured on a neighboring AP in FortiGate.
- Pre-shared Key: Enter the pre-shared key for the SSID.
- Protocol: Select the protocol, **TCP** or **UDP**.
- iPerf Server: Enter iPerf server details. iPerf server generates TCP and UDP data streams which can be used to measure throughput.
- Port: Enter the port number.
- Throughput(MB/s): Enter throughput value in MB/s.

Note: Throughput(MB/s) field is displayed only when **Configured** is selected as baseline type.

4. Click **Add**.

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

Baseline test details						
Name = base_24 × + Q Search Q						
Name ⌵	AP name ⌵	SSID ⌵	Radio ID ⌵	Band ⌵	Channel ⌵	Packet Loss ⌵
Base_24		sam_1	2	5GHz	36	100%

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

Schedule Tests

The tests are the central activity of the SAM application that is dealt the most. A baseline test is performed occasionally, but the scheduled tests and their results are monitored constantly.

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

Add a Scheduled Test

To add a Scheduled Test, follow these steps:

1. Navigate to **Service Assurance>Schedule**.
2. Click **+ Add**.
3. Provide the following details:
 - a. Enter a name for the test.
 - b. Select Test Type, either **Connectivity** or **Throughput**.
Note: Based on the test type selection the advanced options filed changes.
 - c. Select a device.
 - d. Select a Baseline test.
 - e. Select Interval. **Instant** option enables to run the scheduled test once, immediately after it is saved.
Continuous option enables to execute the scheduled test continuously till you disable the test.

4. Configure Advance Options:

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

Field	Description
Packet Loss Good Threshold	Type a value for Packet Loss Good Threshold. If the measured packet loss is above this threshold and baseline, the test result is classified as <i>Bad</i> . If it falls between the threshold and the baseline, it is considered <i>Fair</i> , while values below the threshold and baseline are categorized as <i>Good</i> .

Add baseline test

Details

Name

Testbaseline

Test Type

Connectivity Throughput

Device

FGT-latest-version

AP Radios

F432FRTF23000305-3

+

Baseline Type

Configured Measured

SSID

SAM_SSID

Pre-shared Key

••••••••

Packet Loss(%)

0

Ping Server

8.8.8.8

Important Note:
clicking on "Add" will result in following changes to your WLAN Network, which will impact connected clients on Forti AP.

- New FortiAP Profiles will be created to run Service Assurance Tests
- Baseline Test will be **executed immediately**.

Are you sure you want to proceed?

 Advanced Options

Packet Loss Good Threshold(%)

0

Redo Failed Tests

☒

Retires

2

- If Throughput is selected as Test Type , you can configure the following fields:

Field	Description
Protocol	Select TCP or UDP.
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 <i>Good</i> . If it falls between the threshold and the baseline, it is considered <i>Fair</i> , while values below the threshold are categorized as <i>Bad</i> .

Add new schedule test.

Details

Name

Test Type

Connectivity

Throughput

Device

Baseline Test

Interval

Instant

Continuous

Advanced Options

Protocol

TCP

UDP

Throughput Good Threshold (MB/s)

Important Note:
clicking on "Add" will result in following changes to your WLAN Network, which will impact connected clients on Forti AP.

- New FortiAP Profiles will be created to run Service Assurance Tests
- Schedule Test will be **executed immediately**.

Are you sure you want to proceed?

To delete a schedule, select a schedule from the list and click **Delete**.

To start a scheduled test, click start test icon under **Actions** field. To stop a running scheduled test, click stop test icon under **Actions** field.

Name	SSID	Test Type	Device Name	Baseline	Status	Interval	Action
Thput_UDP_2	sam_1	Throughput	FGT-latest-version	Throughput_UDP_HA	Running	Continuous	Stop
Thput_TCP_2	sam_1	Throughput	FGT-latest-version	Thput_TCP_HA	Stopped	Continuous	Start

