

User Guide

FortiAI Ops 1.1.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change log	4
Overview	5
Service Level Assurance (SLA)	6
Recommended Resources	9
Getting Started	10
ADOM and Non-ADOM Modes	10
Enabling the ADOM Mode	10
Disabling the ADOM Mode	10
Role Based Access	11
Log Forwarding	11
Enabling FortiAI Ops	13
Device Management	14
Licensing	14
Adding and Managing FortiGate Controllers	14
SLA Configurations	16
Device Health	17
Time To Connect	18
Roaming	20
SD-WAN	23
Monitor	25
Overview	25
Summary	28
Top 3 Impacted Sites	30
Wireless	30
Switching	54
WAN	58
Impacted Devices	62
Impacted SLA	65
Administration	67
Upgrading Firmware	67
Diagnostics	68
Special Notes	69

Change log

Date	Change description
2022-12-22	FortiAI Ops 1.1.1 release version.

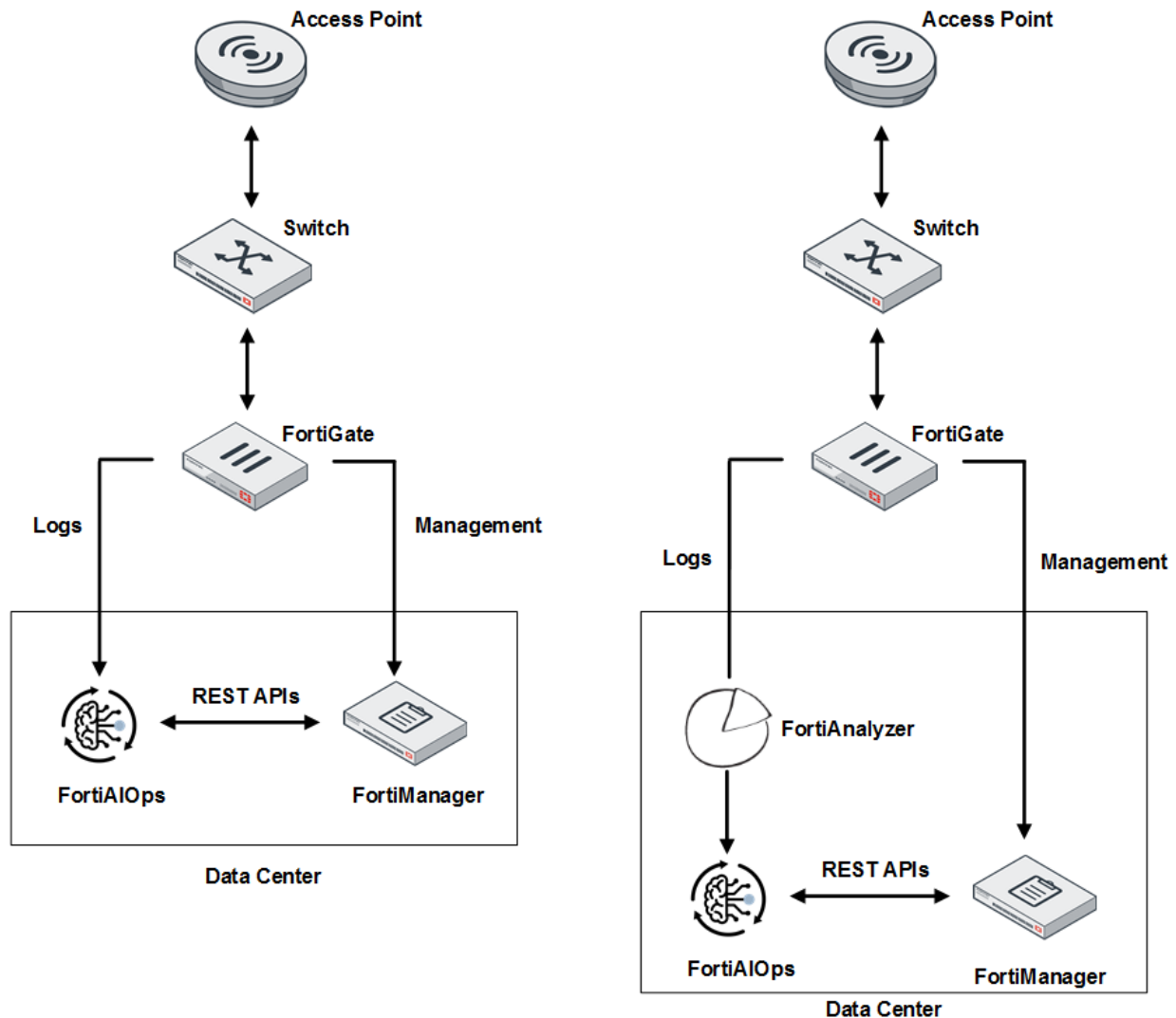
Overview

FortiAI Ops aims at diagnosing and troubleshooting network issues by analyzing potential problems and suggesting remedial steps based on the Artificial Intelligence (AI) and Machine Learning (ML) architecture that it is built upon. FortiAI Ops learns from your network data to report statistics on a comprehensive and simple dashboard, providing network visibility and deep insight into your network. Thus, enabling you to effectively manage your connected devices and resolve network issues swiftly with the help of AI/ML.

FortiAI Ops processes event logs from FortiGate and predicts issues, it also reviews FortiGate configurations periodically for diagnostic and troubleshooting purposes. The data is displayed in the FortiAI Ops user interface that supports screen size of 1024x768, 1280x800, 1366x768, 1920x1080, and also mobile devices' screens.

The FortiAI Ops tool provides the following advantages.

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



The FortiAI Ops Management Extension Application (MEA) container is hosted on the FortiManager integrated platform that provides centralized management of Fortinet products and other devices. For more information on FortiManager operations, see related [product documentation](#).

Service Level Assurance (SLA)

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 to report network issues. You can view the impacted SLA data in the [Monitor](#) dashboards.

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

Wireless

The following SLAs are monitored for wireless clients.

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

Throughput

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

Coverage

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

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. To configure the thresholds, see [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. To configure the thresholds, see [Time To Connect](#).

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. FortiAIOps displays relevant SLAs under different sections on the monitor dashboard. To configure the thresholds, see [Device Health](#).

Switching

The switching SLAs monitor the switch health and connection status.

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

Switch Health and Uptime

The **Switch Health and Uptime** SLA determines the health of the switches based on the configured thresholds (CPU, memory, temperature) and events such as port *down*, switch *down* and so on. FortiAIOps displays relevant SLAs under different sections on the monitor dashboard. To configure the thresholds, see [Device Health](#).

Switch Connection Failure

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

WAN

WAN section comprises monitoring of SD-WAN Performance SLA and FortiExtender based failures.

SD-WAN is a software-defined approach to managing Wide-Area Networks (WAN). It allows you to offload internet bound traffic, that is, private WAN services remain available for real-time and mission critical applications. This added flexibility improves traffic flow and reduces pressure on the network. WAN has member interfaces and ports that are used to run traffic.

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

Performance

You can configure **Performance** SLAs to monitor member interface link quality and to detect link failures. The link quality is measured based on latency, jitter, and packet loss. FortiAIOps WAN SLA can follow the performance SLAs defined on FortiGate and report the SLA breaches. Alternately, you can configure thresholds for these link quality parameters (latency, jitter and packet loss) in FortiAIOps for SLA monitoring. The thresholds can be configured statically or dynamically by FortiAIOps using machine learning algorithms, to identify optimal threshold values for the link parameters. To configure SLA, see [SD-WAN](#).

FortiExtender

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

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

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

Recommended Resources

The following are the recommended resource requirements for FortiAIOps. For more information, see the [FortiManager Release Notes](#).

Maximum devices (FortiGate/FortiSwitches/FortiExtenders/APs/Clients)	Recommended Hardware (FortiManager)
30/30/30/60/600	4 CPU/16 GB RAM/500 GB storage
100/100/300/200/4000	6 CPU/16 GB RAM/500 GB storage
600/600/600/1200/24000	8 CPU/32 GB RAM/2 TB storage
1600/1600/1200/3200/64000	16 CPU/64 GB RAM/2 TB storage
3200/3200/3200/6400/128000	32 CPU/128 GB RAM/2 TB storage

Getting Started

This section provides a summary of how to get started with FortiAI Ops.

- [ADOM and Non-ADOM Modes on page 10](#)
- [Role Based Access](#)
- [Log Forwarding](#)
- [Enabling FortiAI Ops on page 13](#)

ADOM and Non-ADOM Modes

You can manage FortiAI Ops in the ADOM or non-ADOM mode. For more information on creating and managing ADOMs, see the *FortiManager Administration Guide*.

Notes:

- In the ADOM mode, you can add FortiGate controllers managed by the particular ADOM of the FortiManager. FortiAI Ops configures and displays data for only the devices managed by the particular ADOM.
- In the non-ADOM mode, you can add any FortiGate controllers managed by FortiManager.
- If you move a FortiGate controller to a different ADOM, then it is directly managed in the new ADOM.

After you add FortiGates to FortiAI Ops, it communicates with FortiManager to obtain data.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by super user administrators.

Enabling the ADOM Mode

To enable the ADOM mode, log in to the FortiManager as a super user administrator.

1. Go to **System Settings > Dashboard**.
2. In the **System Information** widget, toggle the **Administrative Domain** switch to **ON**.
You will be automatically logged out of the FortiManager and returned to the log in screen.

Disabling the ADOM Mode

To disable the ADOM Mode, you are required to remove all the devices from non-root ADOMs. That is, add all devices to the root ADOM.

1. Delete all non-root ADOMs.
Only after removing all the non-root ADOMs can ADOMs be disabled.
2. Go to **System Settings > Dashboard**.
3. In the **System Information** widget, toggle the **Administrative Domain** switch to **OFF**.
You will be automatically logged out of the FortiManager and returned to the log in screen.

Note: The ADOMs feature cannot be disabled if ADOMs are still configured and have managed devices in them.

Role Based Access

The access privileges to FortiAI Ops are defined as per permissions configured in the administrator profile on FortiManager. For more information, see [Creating administrator profiles](#).

If *Extension Access* is **Read-Only** in the administrator profile, then the following features are not enabled.

- Applying licenses (**Devices > Upload License**)
- Device management (**Devices > FortiGate > Add/Auto-Import/Delete**)
- SLA configurations (**Configuration > Service Level Assurance**)
- Firmware upgrade (**Administration > Firmware Upgrade**)

Log Forwarding

FortiAI Ops supports direct FortiGate log forwarding and FortiAnalyzer log forwarding.

- Direct FortiGate log forwarding - Navigate to **Log Settings** in the FortiGate GUI and specify the FortiManager IP address.

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager ☒ Enabled ☐ Disabled

Send logs to syslog ☒

IP Address/FQDN

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

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager ☒ Enabled ☐ Disabled

Server

Connection status ☒ Connected

Storage usage	<div><div></div></div> 13%	6.30 GiB / 50.00 GiB
Analytics usage	<div><div></div></div> 14%	4.92 GiB / 35.00 GiB
Archive usage	<div><div></div></div> 9%	1.38 GiB / 15.00 GiB

Upload option ☒ Real Time ☐ Every Minute ☐ Every 5 Minutes

Allow access to FortiGate REST API ☒

Verify FortiAnalyzer certificate ☒

Navigate to **Log Forwarding** in the FortiAnalyzer GUI, specify the FortiManager **Server Address** and

select the FortiGate controller in **Device Filters**.

Create New Log Forwarding

Name	FortiAIOps	
Status	<input checked="" type="checkbox"/> ON	
Remote Server Type	<input type="radio"/> FortiAnalyzer <input checked="" type="radio"/> Syslog <input type="radio"/> Common Event Format(CEF)	
Server IP	<input type="text" value="192.168.1.1"/>	
Server Port	<input type="text" value="514"/>	
Reliable Connection	<input type="checkbox"/> OFF	

Log Forwarding Filters

Device Filters	FGT60E-144-240	
	<input type="button" value="Select Device +"/>	
Log Filters	<input type="checkbox"/> OFF	
Enable Exclusions	<input type="checkbox"/> OFF	

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

FortiManager Syslog Configurations

You are required to add a Syslog server in FortiManager, navigate to **System Settings > Advanced > Syslog Server**. Enter the name, IP address or FQDN of the syslog server (localhost), and the port.

Create New Syslog Server Settings

Name	FortiAIOps
FQDN/IP	localhost
Syslog Server Port	514
Reliable Connection	<input checked="" type="checkbox"/>

Additionally, configure the following Syslog settings via the CLI mode.

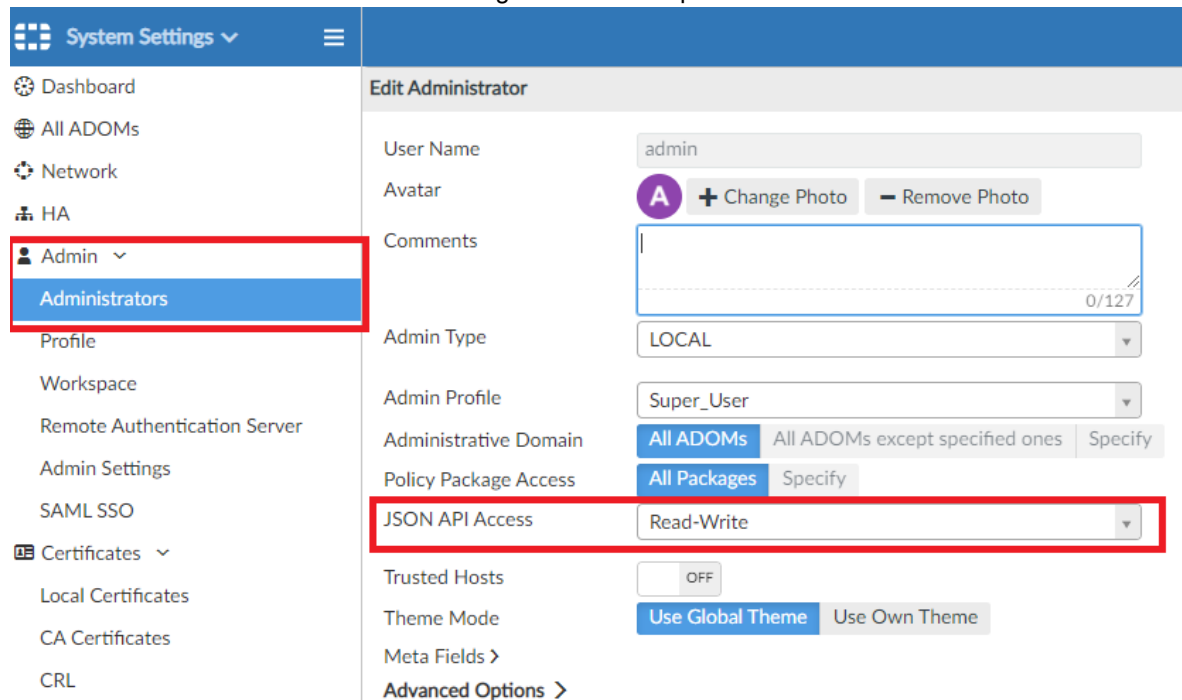
```
config system locallog syslogd3 setting
    set severity information
    set status enable
    set syslog-name "FortiAIOps"
end
```

For more information on configuration described in this section, see the FortiManager *Administration Guide* and *Log Message Reference*.

Enabling FortiAIOPS

Follow this procedure to enable FortiAIOPS.

1. Connect to the FortiManager GUI.
2. Navigate to **System Settings > Administrators > Admin** and set **JSON API Access** to **Read-Write**. This enables communication between FortiManager and FortiAIOPS.



The screenshot displays the FortiManager GUI. On the left, the 'System Settings' menu is expanded, showing 'Admin' and 'Administrators' under the 'Admin' section. The main content area is titled 'Edit Administrator' and shows the configuration for the 'admin' user. The 'JSON API Access' dropdown is set to 'Read-Write' and is highlighted with a red box. Other visible settings include 'User Name' (admin), 'Avatar' (A), 'Comments' (0/127), 'Admin Type' (LOCAL), 'Admin Profile' (Super_User), 'Administrative Domain' (All ADOMs), 'Policy Package Access' (All Packages), 'Trusted Hosts' (OFF), 'Theme Mode' (Use Global Theme), and 'Meta Fields' (Advanced Options >).

3. Navigate to **Management Extensions** and click the **FortiAIOPS** tile.



Note: Ensure that the DNS server is reachable.

Device Management

This section describes managing licensing and FortiGate controllers.

- [Licensing](#)
- [Adding and Managing FortiGate Controllers](#)

Licensing

FortiAIOPS licensing quota is based on the number of managed FortiGate controllers. FortiAIOPS base license allows managing 10 FortiGate controllers. For additional licensing requirements, contact the *Fortinet Customer Support* with the **System ID** displayed on the **Licenses** page or register with FortiCare.

Navigate to **Devices > FortiGate** to access the **Licenses** page. The **Available Licenses** tab indicates the number of active licenses available for use with FortiAIOPS and the **Unlicensed Devices** tab indicates the number of unlicensed devices in FortiAIOPS.

Note: An unlicensed version of FortiAIOPS allows managing only one FortiGate controller.

To upload the license file, click **Upload License** and navigate to the **.lic** file.

LICENSES (System ID: c243385362768d2e00bac66ce7c992bf) Available Licenses: 13 Unlicensed Devices: 0

Upload License File (.lic) Choose File Lic248-demo.lic

OK Cancel

The license file is displayed with associated details such as license validity (start and expiry dates), the number of licenses and the uploaded license file name.

LICENSES (System ID: c243385362768d2e00bac66ce7c992bf) Available Licenses: 13 Unlicensed Devices: 0

Upload License Search

Feature	File Name	Start Date	Expiry Date	Number of Licenses
AIOPS-BASE	new_license_224.lic	30-Aug-2021	30-Aug-2022	20
AIOPS-BASE	Default License	11-Aug-2021	Permanent	1

Note: Ensure that the WAN monitoring license is applied to the FortiGate controller to generate congestion logs.

Adding and Managing FortiGate Controllers

You can import the FortiGate controllers from the FortiManager device database. In the ADOM mode, you can add FortiGate controllers managed by the particular ADOM and in the non-ADOM mode, you can add any controller managed by FortiManager. See section [ADOM and Non-ADOM Modes on page 10](#). For details about adding model devices to FortiManager, see the *FortiManager Administration Guide*.

All FortiAPs and FortiSwitches managed by the imported controller are monitored by FortiAIOPS. Navigate to **Devices > FortiGate** and in the **Device (s)** section.

DEVICE(S)

[Add](#)
[Auto Import](#)
[Delete](#)
[Refresh](#)
[+ Search](#)


FortiGate Serial	Host Name	IP Address	Model	Software Version	Availability State	HA Mode
FGVM64-101F	FGVM64-101F	10.10.10.10	FGVM64	v7.2.3	Online	Standalone
FGT61E-101F	FGT61E-101F	10.10.10.10	FGT61E	v7.2.5	Online	Standalone

To manually add a FortiGate controller, click **Add** and select the FortiGate controllers in **Device Selection**.

DEVICE(S)

Device Selection

OK Cancel


Devices  FortiGate-101F

IP Address 10.10.10.10

Serial Number FGVM64-101F

Devices (1)

Fortigate (1)

 FortiGate-101F

The added FortiGate controller is now listed.

You can also automatically import the FortiGate controllers from FortiManager. Click **Auto Import** and you can enable the automatic import of associated FortiGate controllers into all or selected ADOMs.

DEVICE(S)

Auto Import Options are Disabled Enabled for All Enabled Selected

Select a device and click **Delete** to delete the selected controller from FortiAIOps.

You can import FortiGate clusters in FortiAIOps, the HA configuration (Active-Active/Active-Passive) is preserved and the **HA Mode** is displayed in the **Device(s)** panel.

SLA Configurations

This section explains how to configure SLA metrics to define values to match network deployment and required thresholds.

- [Device Health](#)
- [Time To Connect](#)
- [Roaming](#)
- [SD-WAN](#)



Device Health




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




Navigate to **Configuration > Service Level Assurance > Device Health** to configure the following parameters.

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

- **Temperature**

AP Health		
CPU	<input type="text" value="1"/>	(%)
		<input type="button" value="Low"/>
Memory	<input type="text" value="1"/>	(%)
		<input type="button" value="Low"/>

Switch Health		
CPU	<input type="text" value="1"/>	(%)
		<input type="button" value="Low"/>
Memory	<input type="text" value="1"/>	(%)
		<input type="button" value="Low"/>
Temperature	<input type="text" value="64.4"/>	(°C)
		<input type="button" value="Medium"/>

FortiExtender Health		
CPU	<input type="text" value="35"/>	(%)
		<input type="button" value="Medium"/>
Memory	<input type="text" value="36"/>	(%)
		<input type="button" value="Medium"/>
Temperature	<input type="text" value="22"/>	(°C)
		<input type="button" value="Low"/>

The default value for the CPU and memory parameters is 60% and the default value for the temperature is 64.4 degree Celsius.

Time To Connect

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

displayed in the [Monitor](#) tab.

Navigate to **Configuration > Service Level Assurance > Time to Connect**.

Dynamic Baselines

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

SLA CONFIGURATIONS

Device Health
Time to Connect
Roaming
SD-WAN

☒ Dynamic Baselines Configuration

Scope

Adom
FortiGate
AP

Time Selection

Duration
Date Range

7 Day(s)

Schedule Baselines Computation
☒

14-07-2022
2

Repeat Cycle
☒

7
Day(s)

OK
Cancel

DYNAMICALLY OBTAINED BASELINES VALUES

Refresh
Recompute Baselines
+ Q Search

Last Updated	AP Name	FortiGate Hostname	Association	Authentication Time	DHCP Time	DNS Time	Status
2022/07/07 15:23:26	XXXXXXXXXX	XXXXXXXXXX	6ms	10ms	2s 12ms	0ms	Computation of Dynamic Thre
2022/07/07 15:23:33	XXXXXXXXXX	XXXXXXXXXX	2ms	7ms	2ms	0ms	Computation of Dynamic Thre
2022/07/07 15:23:33	XXXXXXXXXX	XXXXXXXXXX	300ms	300ms	300ms	0ms	No data available for selected

- **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.

SLA CONFIGURATIONS

Device Health
Time to Connect
Roaming
SD-WAN

☒ Dynamic Baselines Configuration

Association Time
212015
ms

Low

Authentication Time
74084
ms

Low

DHCP Time
137302
ms

Low

DNS Time
300
ms

Low

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

Note: 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 [Monitor](#) tab.

Navigate to **Configuration > Service Level Assurance > Roaming**.

Dynamic Baselines

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

SLA CONFIGURATIONS

Device Health Time to Connect **Roaming** SD-WAN

Dynamic Baselines Configuration

Scope Adom **FortiGate** AP SSIDTime Selection **Duration** Date Range

1 Day(s)

Schedule Baselines Computation ☒ 14-07-2022 20Repeat Cycle ☐

OK

Cancel

DYNAMICALLY OBTAINED BASELINES VALUES

Refresh Recompute Baselines Search

Last Updated	FortiGate Hostname	11r Time	OKC Time	PMK Time	Status
2022/07/13 16:54:14	FortiGate-300E	55ms	100ms	100ms	No data available for selected range, Hence using older dy...
2022/07/13 16:54:14		55ms	100ms	100ms	No data available for selected range, Hence using older dy...
2022/07/13 16:54:14		55ms	100ms	100ms	No data available for selected range, Hence using older dy...

- **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.

SLA CONFIGURATIONS

Device Health
Time to Connect
Roaming
SD-WAN

☒ Dynamic Baselines Configuration

Fast BSS Transition Roams(11r)

Opportunistic Key Caching Roams(okc)

PMK Cache Roams

ms

ms

ms

Low

Low

Low

- **Fast BSS Transition Roams(11r)** - This is implemented as part of the 802.11r standard and enables fast roaming of wireless clients by pre-authenticating them with several APs in the network; this pre-authentication is done prior to when the client begins roaming. This feature allows immediate BSS transitions between APs and curtails the latency caused by deferred data connectivity, often experienced when a client has to transition from one BSS to another while roaming in a multi-AP deployment. The default roaming time value is 55 ms and the valid range is 1 - 600000 ms.

Note: To use this feature of 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.

FortiAI Ops 1.1.1 User Guide
Fortinet Inc.

22

SD-WAN

You can configure the SD-WAN SLAs in FortiAI Ops or in FortiGate. Navigate to **Configuration > Service Level Assurance > SD-WAN**. The following configurations are *required* in FortiGate to receive SD-WAN logs.

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

Dynamic Baselines

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

SLA CONFIGURATIONS

Device Health
Time to Connect
Roaming
SD-WAN

Dynamic Baselines Configuration

Scope
FortiGate
Interface
SLA

Time Selection
Duration
Date Range

1 Hour(s)

Schedule Baselines Computation
19-07-2022
20

Repeat Cycle
7
Hours(s)

OK
Cancel

DYNAMICALLY OBTAINED BASELINES VALUES

Refresh
Recompute Baselines
Search

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

- **Scope** - Select the scope to calculate the thresholds which could either be per **FortiGate**, per **Interface**, or per **SLA**.
- **Time Selection** - Set the time range/duration for which 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

Select **Baseline** to configure the threshold configuration criteria in FortiAI Ops or **FortiGate** to use the settings configured in FortiGate. For more information, see the [SD-WAN minimum SLA configuration](#).

SLA CONFIGURATIONS

Device HealthTime to ConnectRoamingSD-WAN

☒ Dynamic Baselines Configuration

Baselines TypeBaselineFortiGate

Jitter100ms

Low

Packet Loss20%

Low

Latency100ms

Low

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

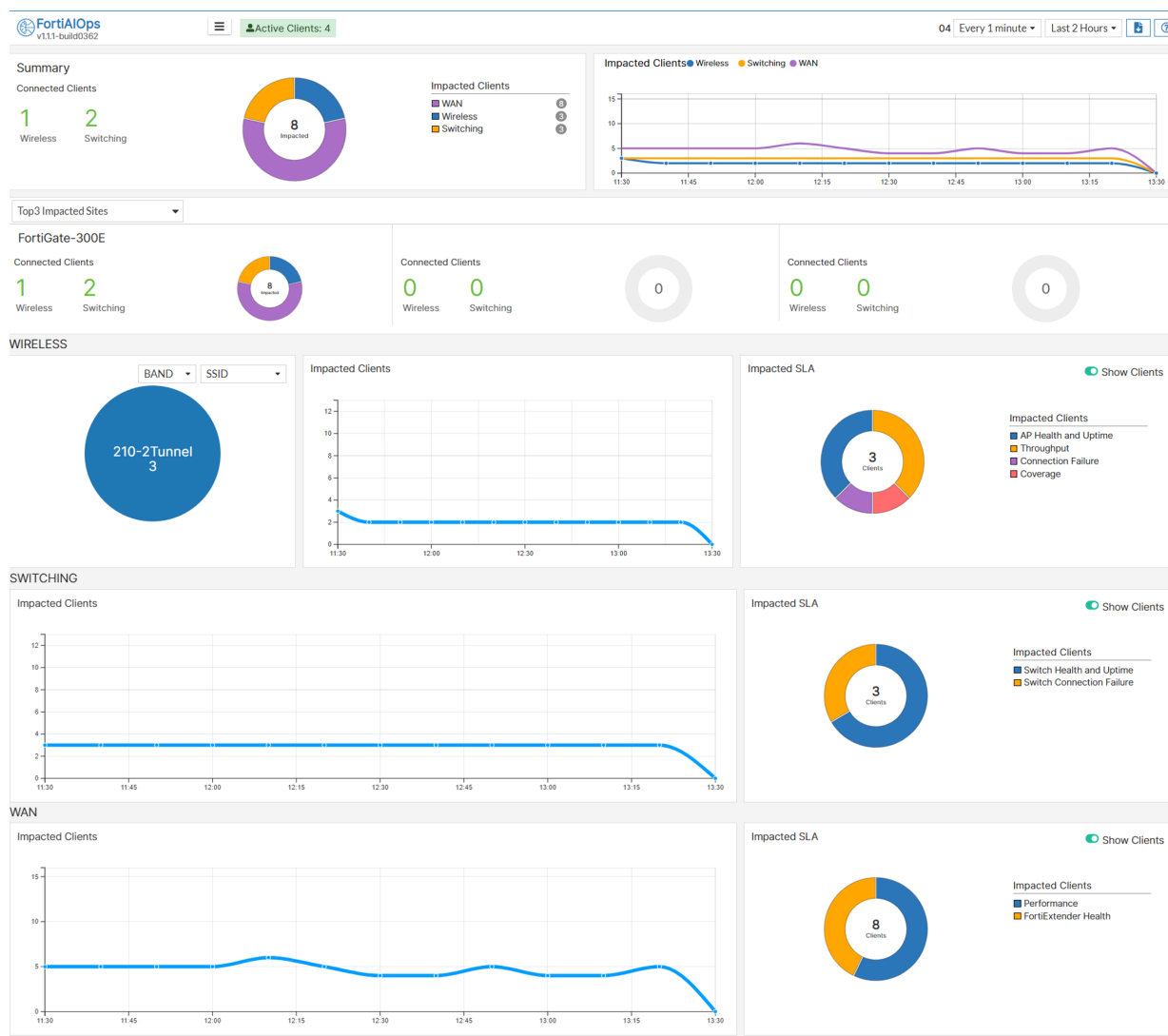
Monitor

The FortiAI Ops provides a comprehensive dashboard with detailed statistics and visualization for the wireless, switching, and WAN clients. The information presented in the dashboard for impacted clients is pivotal for monitoring device health for diagnostic purpose.

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

Overview

The overview dashboard present data in five panels - **Summary**, **Top 3 Impacted Sites**, **Wireless**, **Switching**, and **WAN**. Data is displayed in a series of charts and graphs, that you can filter based on time duration. Navigate to **Monitor > Overview**.



The total number of **Active Clients** is displayed in this page, indicating the total number of clients that are currently connected (since 4 minutes). Click on the active client count to view details of active wireless and switching clients.

Active Clients Details

Wireless (3) Switching (4)

View details

+ Search

Association time	Client Mac Address	FortiGate Hostname	AP Name	SSID	Channel
2022/07/04 15:11:04	98:77:18:00:00:00	FortiGate-101F	FP431FTF20010590	Alops_tunnel	165
2022/07/04 15:10:43	78:25:17:00:00:00	FortiGate-101F	FP431FTF20010590	AI_RSSI	165
2022/06/04 19:58:58	98:77:18:00:00:00	FortiGate-101F	FP431FTF20010590	AI_RSSI	165


Active Clients Details

Wireless (3) Switching (4)

Search

Association time	Client Mac Address	FortiGate HostName	Switch Name	Port
2022/07/06 15:17:42	98:6B:47:7A:7A:08	FGT0000000000000000	SS-0000000000000000	port7
2022/07/06 15:17:42	98:6B:47:7A:7A:08	FGT0000000000000000	SS-0000000000000000	port11
2022/07/06 15:17:42	98:6B:47:7A:7A:08	FGT0000000000000000	SS-0000000000000000	port21
2022/07/06 15:17:42	98:6B:47:7A:7A:08	FGT0000000000000000	SS-0000000000000000	port11

Select a specific client and click on **View Details**, the detailed summary of the selected client is displayed.

Client Details	
Device Name	 Galaxy-Note9
MAC Address	98:6B:47:7A:7A:08
Association Time	2022/07/18 14:36:21
AP Name	FP-83x-3F-CNTRLR_Dev
FortiGate Hostname	office-wifi-qa
Channel	60
Radio Type	5GHz 802.11ac/n/a
AP Serial	FGT0000000000000000
AP IP Address	192.168.1.100
FortiGate Serial	FGT0000000000000000
FortiGate IP Address	192.168.1.1
MIMO	2x2

General

-60 dBm

Signal Strength

-95 dBm

Noise

5 GHz

Band

35 dB

SNR

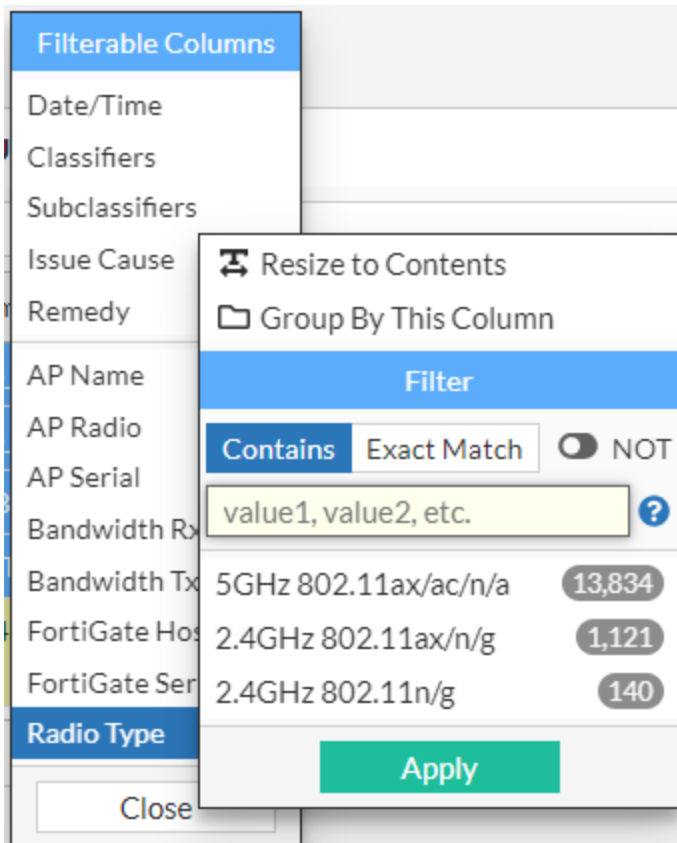
0%

Transmission Discard

0%

Transmission Retry

The data displayed in tabular format in all the monitor dashboard pages is filterable based on columns, you can group data by a specific column or filter data for specific values. This is an example.

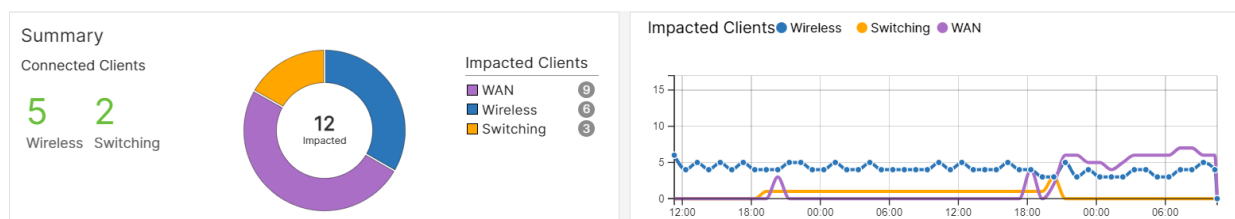


Dashboard data is refreshed at a configurable interval.

- [Summary](#)
- [Top 3 Impacted Sites](#)
- [Wireless](#)
- [Switching](#)
- [WAN](#)

Summary

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



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

Connected Wireless Clients Details ✕					
View details + <input type="text" value="Search"/>					
Association time	Client Mac Address	FortiGate Hostname	AP Name	SSID	Channel
2022/07/04 15:11:04	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	Alops_tunnel	165
2022/07/06 10:09:21	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	1B_sys_tb	144
2022/07/06 10:04:53	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	1B_sys_tb	144
2022/07/05 15:43:50	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	aiops-legacyc	11

This is the client detail for switching.

Connected Switching Clients Details ✕				
+ <input type="text" value="Search"/>				
Association time	Client Mac Address	FortiGate HostName	Switch Name	Port
2022/07/06 15:27:44	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	port7
2022/07/06 15:27:44	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	port11
2022/07/06 15:27:44	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	port21
2022/07/06 15:27:44	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	port11

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

Impacted Clients Details ✕					
Wireless (3) Switching (4) SD-WAN (0)					
View details + <input type="text" value="Search"/>					
Association time	Client Mac Address	FortiGate Hostname	AP Name	SSID	Channel
2022/07/05 13:08:49	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	Alops_tunnel	165
2022/07/05 13:17:45	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	AI_RSSI	165
2022/07/05 13:18:16	88:00:00:00:00:00	FortiGate-101F	FortiGate-101F	AI_RSSI	165

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

Client Details

Device Name	IND-IBASH-NB
Device MAC Address	
Association Time	2022/07/18 12:26:35
AP Name	FP-83x-3F-IT-Bay
FortiGate Hostname	office-wifi-qa
SSID	Forti-Corp-3F-PSK
Channel	44
Radio Type	5GHz 802.11ax/ac/n/a
AP Serial	
AP IP Address	
FortiGate Serial	1
FortiGate IP Address	
Device IP Address	
MIMO	2x2

General

-46 dBm

Signal Strength

-95 dBm

Noise

5 GHz

Band

49 dB

SNR

0%

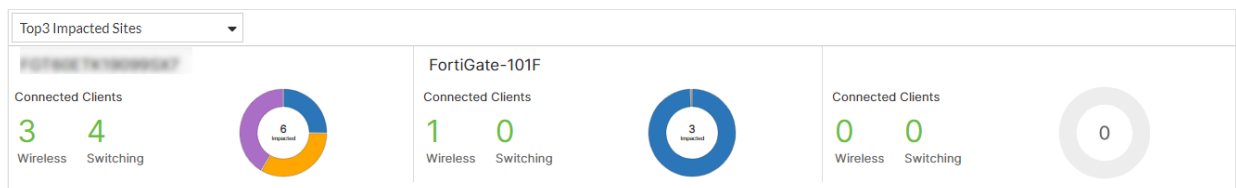
Transmission Discard

0%

Transmission Retry

Top 3 Impacted Sites

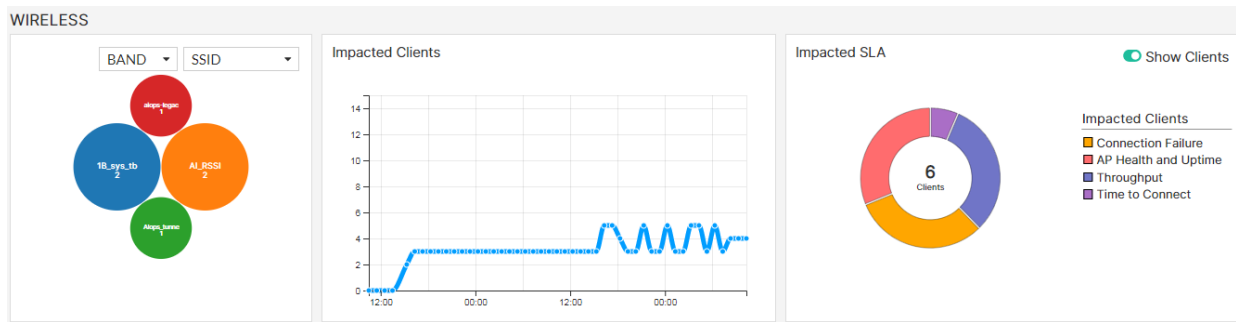
The **Top 3 Impacted Sites** panel allows you to view client data related to the top 3 FortiGate controllers with the highest number of impacted wireless and switching clients. It also displays the total number of connected and impacted clients for each FortiGate controller. You can view collective data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



Wireless

The **Wireless** panel allows you to filter data based on a specific SSID/Band or view the consolidated data for all SSIDs. The total number of impacted wireless clients at different time duration for the selected SSID/Band are

displayed. The *Impacted SLA* data is displayed for impacted clients and/or devices (FortiGate and APs).



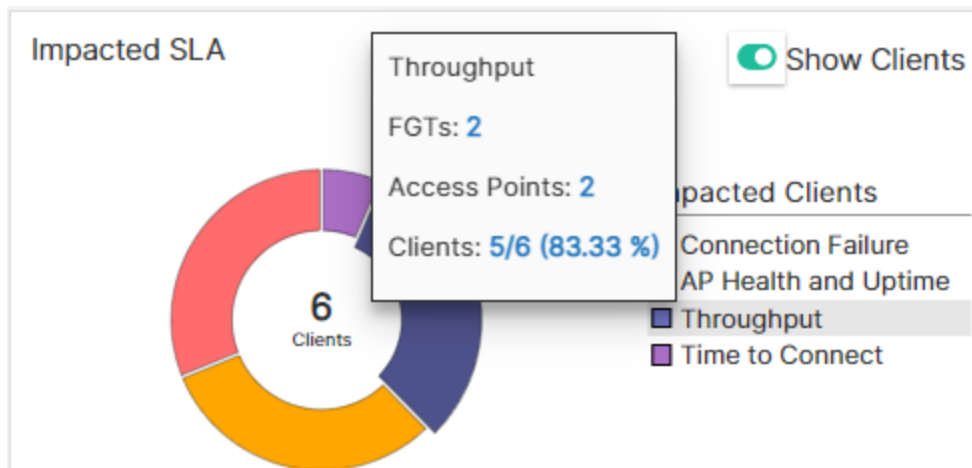
SLAs, Topology, and Logs

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

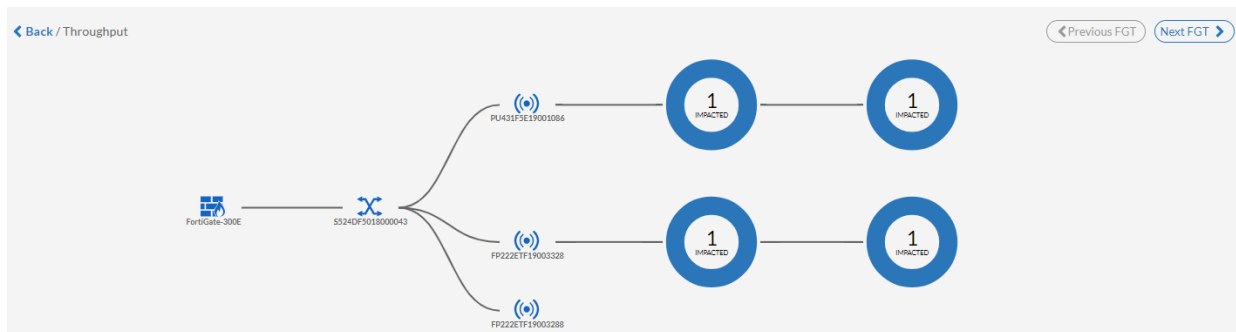
- [Throughput](#)
- [Connection Failure](#)
- [Time to Connect](#)
- [Coverage](#)
- [Roaming](#)
- [AP Health and Uptime](#)

Throughput

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



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



The **Throughput Failures** table displays information such as the impacted radios for the reported classifiers and sub-classifiers, issue description and the suggested remediation measure, and so on are displayed.

THROUGHPUT FAILURES					
View Details + Search					
Date/Time	Radio Type	Classifiers	Subclassifiers	Impacted Clients	Bandwidth
FP431FTF20008908 10					
2022/07/05 17:20:54	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	21.28 Kbps
2022/07/05 15:57:53	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	7.70 Kbps
2022/07/05 15:55:53	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	6.28 Kbps
2022/07/05 15:53:53	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	7.69 Kbps

Resize Columns to Content

Reset Table

Select Columns

✓

Date/Time

✓

Radio Type

✓

Classifiers

✓

Subclassifiers

✓

Impacted Clients

✓

Bandwidth Tx

✓

Bandwidth Rx

AP Radio

AP Serial

FortiGate Hostname

FortiGate Serial

Issue Cause

Remedy

Apply

Cancel

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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Impacted Clients	The number of impacted clients.
Issue Cause	Detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
AP Radio	The AP radio that the client associated with.
AP Serial	The AP serial number that the client associated with.
Bandwidth Rx	The Rx data throughput of the impacted AP.
Bandwidth Tx	The Tx data throughput of the impacted AP.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
Radio Type	The impacted radio and band information.

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

Throughput Logs

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	<ul style="list-style-type: none"> 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 - 852-40P5018000043 (port17)
Remedy	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Asymmetric uplink and downlink rates for some clients; likely due to asymmetric power/high channel contention/retries
Remedy	<ul style="list-style-type: none"> 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.

Logs

Description

Radio Info

Radio Type	Bandwidth Tx	Bandwidth Rx	Channel Utilization(%)	Client Count	Oper Chan	Oper Tx Power
802.11ax-5G	795.27 Kbps	113.15 Kbps	20	11	60	15 dBm

1

Wired Status

Interface	Full Duplex	Link Speed(mbps)	bytes Rx	bytes Tx	Collisions	Dropped Rx	Dropped Tx
lan1	true	1000	442456927813	154860226111	0	762954	0

AP Logs

This tab provides the AP event logs generated from FortiGate.

Event Time	AP	Action	Message	LogDesc
2022/05/24 13:19:04	FP-83x-3F-EzRF_Dev	DHCP6-SOLICIT	DHCP6 SOLICIT from client 00:93:37:e9:...	Wireless station sent DHCP6 SOLICIT
2022/05/24 13:19:03	FP-83x-3F-EzRF_Dev	DHCP6-SOLICIT	DHCP6 SOLICIT from client 00:93:37:e9:...	Wireless station sent DHCP6 SOLICIT
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	auth-req	AP received authentication request frame ...	Authentication request from wireless
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	auth-resp	AP sent authentication response frame to ...	Authentication response to wireless s
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	reassoc-req	AP received reassociation request frame f...	Reassociation request from wireless s
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-1/4-key-msg	AP sent 1/4 message of 4-way handshake ...	AP sent 1/4 message of 4 way handsh
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	reassoc-resp	AP sent reassociation response frame to cl...	Reassociation response to wireless st
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-2/4-key-msg	AP received 2/4 message of 4-way handsh...	Wireless client sent 2/4 message of 4
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-3/4-key-msg	AP sent 3/4 message of 4-way handshake ...	AP sent 3/4 message of 4 way handsh
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-4/4-key-msg	AP received 4/4 message of 4-way handsh...	Wireless client sent 4/4 message of 4

10

Switch Info

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

Switch Config

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

Neighbour APs

This tab displays coverage hole/distant client issues.

AP Radio	Band	RSSI	RSSI Age
FP231FTF21006576	5 GHz	18	37
FP431FTF20008805	5 GHz	22	38
FP431FTF20008898	5 GHz	16	38

3

WIFI Clients

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

Logs

Description

Date/Time	Client Mac Address	SSID	Radio Type	Classifier	Subclassifier	Signal Strength
2022/05/24 13:23:42	08:00:27:1a:2b:3c	Forti-Corp-3F-PSK	802.11ax-5G	Coverage	Asymmetric Data Rates	-54 dBm
2022/05/24 13:23:42	08:00:27:1a:2b:3c	Forti-Corp-3F-PSK	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	08:00:27:1a:2b:3c	Forti-Corp-3F-PSK	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	08:00:27:1a:2b:3c	Forti-Corp-3F-PSK	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
08:00:27:1a:2b:3c	60	802.11ax-5G	Forti-Corp-3F-PSK	456.00 Mbps	0	642.00 bps
08:00:27:1a:2b:3c	60	802.11ax-5G	Forti-Corp-3F-PSK	12.00 Mbps	0	1.77 Kbps
08:00:27:1a:2b:3c	60	802.11ax-5G	Forti-Corp-3F-PSK	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(dBm)
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-56
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-52
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-47
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-56
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-67
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-56
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-62
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-60
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-60
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-65
2022/05/24 11:02:56	08:00:27:1a:2b:3c	-64

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

[Back](#) / Throughput

IMPACTED CLIENT(S)

Show AP Details Search

Date/Time	Client Mac Address	Device	SSID	Radio Type	Classifier	Subclassifier
FP431FTF20008908 10						
2022/07/05 17:20:54	60:a5:e2:4d:bc:eb	DESKTOP-TJF5KTD	1B_sys_tb	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates
2022/07/05 15:57:53	60:a5:e2:4d:bc:eb	DESKTOP-TJF5KTD	1B_sys_tb	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates
2022/07/05 15:55:53	60:a5:e2:4d:bc:eb	DESKTOP-TJF5KTD	1B_sys_tb	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates
2022/07/05 15:53:53	60:a5:e2:4d:bc:eb	DESKTOP-TJF5KTD	1B_sys_tb	5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates

☒ Resize Columns to Content
☒ Reset Table
Select Columns
☒ Date/Time
☒ Client Mac Address
☒ Device
☒ SSID
☒ Radio Type
☒ Classifier
☒ Subclassifier
☒ Signal Strength
☒ Tx Rate
☒ Rx Rate
☐ AP Radio
☐ AP Serial
☐ Channel
☐ FortiGate Hostname
☐ FortiGate Serial
☐ Max Capacity
☐ SNR

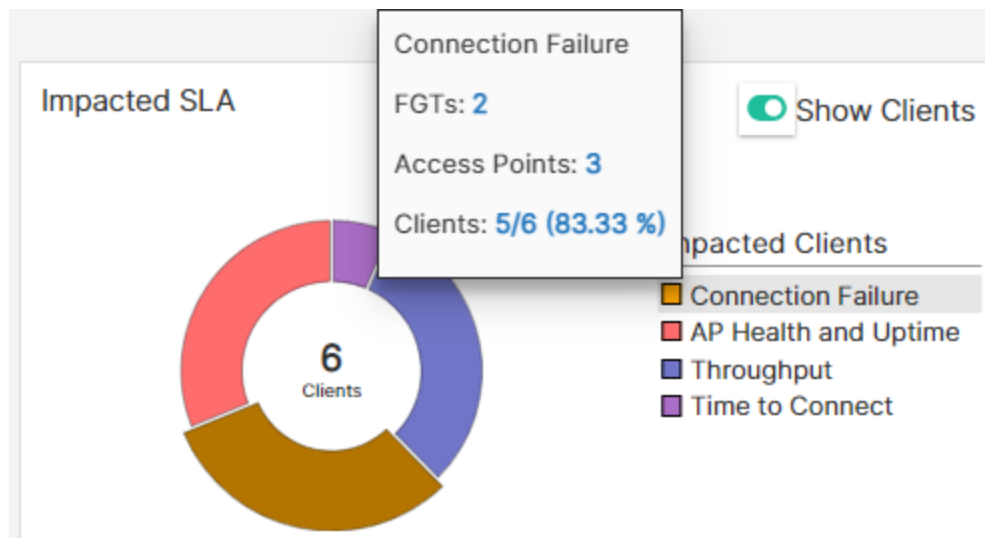
Right-click on the header of the table to select the following columns that you wish to view.

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

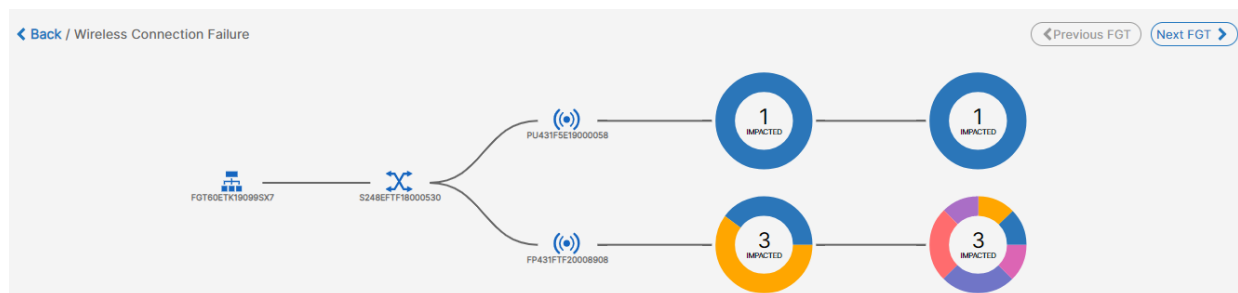
Select any impacted client and click **Show AP details** to view the detailed AP logs. For more details on each of these tabs, see **View Details** in [Throughput](#) logs described earlier in the section.

Connection Failure

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



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



The **Impacted Clients** table displays details such as the client MAC address, the associated AP serial number and the SSID, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on are displayed.

IMPACTED CLIENT(S)							
View Logs Search							
Date/Time	Client Mac Address	Device	SSID	Classifier	Sub Classifier	Issue Cause	
2022/05/16 10:36:45	FP222ETF19003328	DESKTOP-J2D9JHG	210-Bridge	Authentication	Too Many Retries	Too many 802.11 authentication attempts	Rec
2022/05/16 08:00:55	FP222ETF19003328	DESKTOP-J2D9JHG	210-Bridge	Authentication	Incomplete Connection	Wireless client could not complete 802.11 authentication	Rec

Resize Columns to Content
 Reset Table
 Select Columns
☒ Date/Time
☒ Client Mac Address
☒ Device
☒ SSID
☒ Classifier
☒ Sub Classifier
☒ Issue Cause
☒ Remedy
☐ AP Serial
☐ FortiGate Hostname
☐ FortiGate Serial
☐ Sequence Number
☐ User Name
 Apply Cancel

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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.

Attribute	Description
Client MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Signal Strength	The signal strength of the client at the time of impact.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
AP Serial	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
User Name	The impacted client user name.

In the impacted client details displayed for **Connection Failure**, 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 ✕

PU431F5E19000034		2.4GHz	Band
Association Time	2022-07-05 12:30:15	-30dBm	Signal Strength
Channel	11	38dB	Signal Strength/Noise
FortiAP		0%	Transmission Discard
MIMO	2x2	0%	Transmission Retry
SSID	123_tunnel		

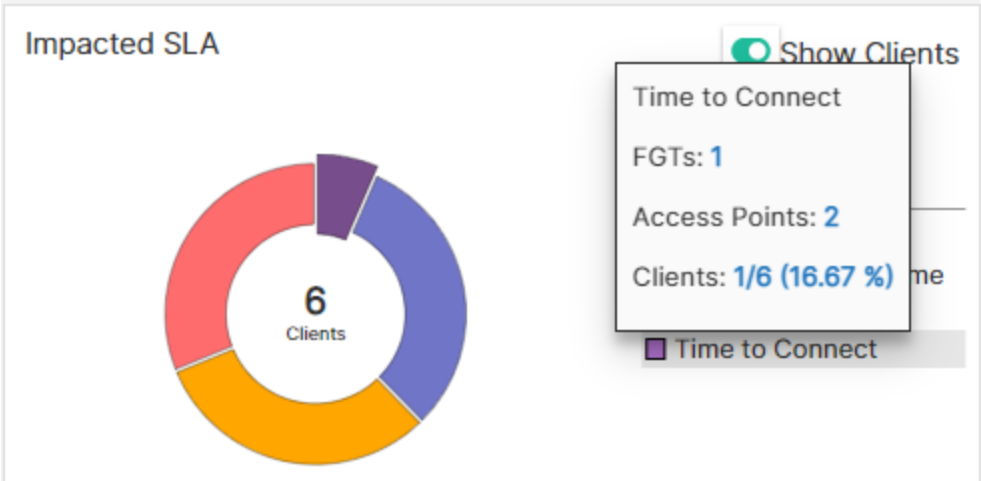
CLIENT LOGS

+ Q Search

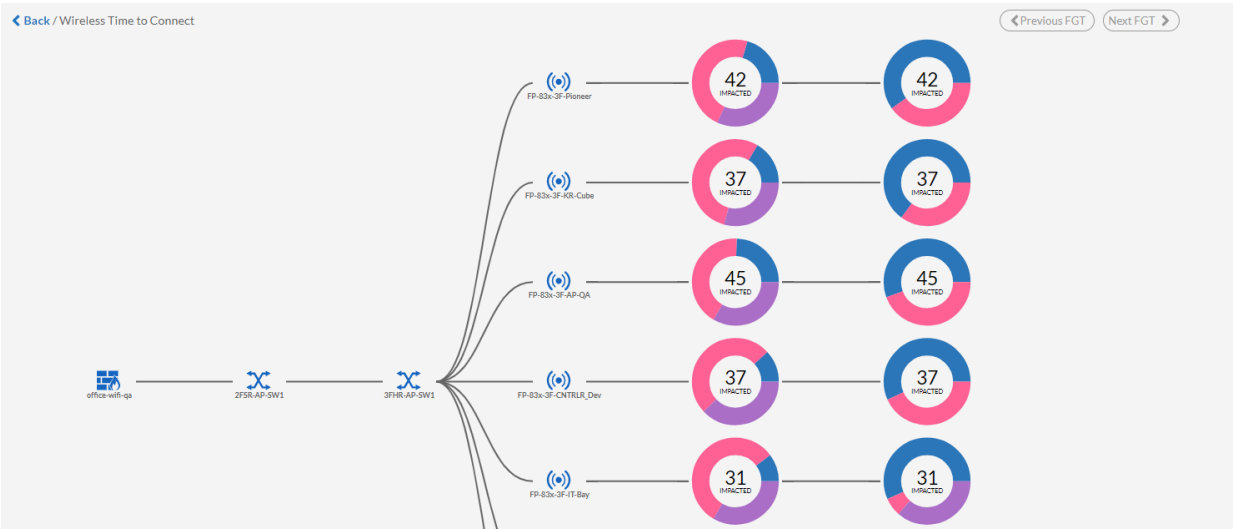
Date/Time ⇅	Level ⇅	Action ⇅	Message ⇅	Channel ⇅
2022/07/06 11:38:17	Warning	DNS-no-resp	DNS server not responding for client 90:27:e...	-

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](#)



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



The **Time to Connect** table displays details such as the client MAC address, the associated AP serial number and the SSID, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on are displayed. In this image impacted client details for **Time to Connect** are displayed.

[Back](#) / Wireless Time to Connect

IMPACTED CLIENT(S)

View Logs [+](#) [Q](#) Search

Date/Time	Client Mac Address	Device	SSID	Classifier	Sub C
PU431F5E19001086 1					
2022/12/19 00:30:23	3c:a9:14:35:68:a4	FTNT-THINK-2	210-2Tunnel	Association	Covera

Select Columns

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

Apply Cancel

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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Client MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Signal Strength	The signal strength of the client at the time of impact.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
AP Serial	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
User Name	The impacted client user name.
Association Delay	The association delay measured in milliseconds.
Authentication Delay	The authentication delay measured in milliseconds.
DNS Delay	The DNS delay measured in milliseconds.
DHCP Delay	The DHCP delay measured in milliseconds.

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

Client Details ✕

FP231FTF21006576		5GHz	Band
Association Time	2022-06-29 20:05:52	-45dBm	Signal Strength
Channel	36	50dB	Signal Strength/Noise
FortiAP	FortiAP-1000000000	0%	Transmission Discard
MIMO	2x2	0%	Transmission Retry
SSID	250-Bridge		

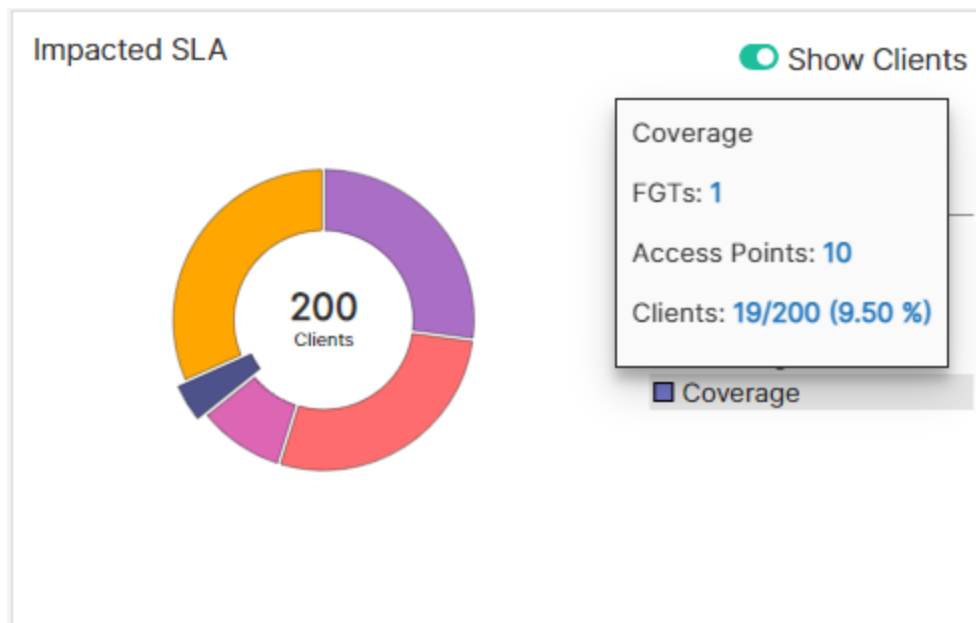
CLIENT LOGS

+ Q Search

Date/Time	Level	Action	Message	Channel
2022/07/05 03:15:25	Notice	DHCP-ACK	DHCP ACK for IP 10.37.107.14 from server 10...	-
2022/07/05 03:15:25	Notice	DHCP-INFORM	DHCP INFORM from client 3c:a9:f4:35:68:d...	-
2022/07/05 03:14:08	Warning	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from c...	-

Coverage

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



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



The **AP Events** table displays issue details such as the radio type, Tx power, neighbour AP count, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on are displayed.

The screenshot shows the 'AP EVENT(S)' table. A right-click context menu is open over the table header, displaying a 'Select Columns' list. The list includes various columns with checkboxes, most of which are checked. The table itself shows a single event with the following details:

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

The 'Select Columns' menu options are:

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

Buttons at the bottom of the menu are 'Apply' and 'Cancel'.

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

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

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

Coverage Logs

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

AP Info	
Name	43x_2F_Cafe_Fridge
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	<ul style="list-style-type: none"> Far off clients connected to the AP
Remedy	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Far off clients connected to the AP
Remedy	<ul style="list-style-type: none"> 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.

Logs

Description

Radio Info

Radio Type	Bandwidth Tx	Bandwidth Rx	Channel Utilization(%)	Client Count	Oper Chan	Oper Tx Power
802.11ax-5G	795.27 Kbps	113.15 Kbps	20	11	60	15 dBm

1

Wired Status

Interface	Full Duplex	Link Speed(mbps)	bytes Rx	bytes Tx	Collisions	Dropped Rx	Dropped Tx
lan1	true	1000	442456927813	154860226111	0	762954	0

AP Logs

This tab provides the AP event logs generated from FortiGate.

Event Time	AP	Action	Message	LogDesc
2022/05/24 13:19:04	FP-83x-3F-EzRF_Dev	DHCP6-SOLICIT	DHCP6 SOLICIT from client 00:93:37:e9:...	Wireless station sent DHCP6 SOLICIT
2022/05/24 13:19:03	FP-83x-3F-EzRF_Dev	DHCP6-SOLICIT	DHCP6 SOLICIT from client 00:93:37:e9:...	Wireless station sent DHCP6 SOLICIT
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	auth-req	AP received authentication request frame ...	Authentication request from wireless
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	auth-resp	AP sent authentication response frame to ...	Authentication response to wireless s
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	reassoc-req	AP received reassociation request frame f...	Reassociation request from wireless s
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-1/4-key-msg	AP sent 1/4 message of 4-way handshake ...	AP sent 1/4 message of 4 way handsh
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	reassoc-resp	AP sent reassociation response frame to cl...	Reassociation response to wireless st
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-2/4-key-msg	AP received 2/4 message of 4-way handsh...	Wireless client sent 2/4 message of 4
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-3/4-key-msg	AP sent 3/4 message of 4-way handshake ...	AP sent 3/4 message of 4 way handsh
2022/05/24 13:19:00	FP-83x-3F-EzRF_Dev	WPA-4/4-key-msg	AP received 4/4 message of 4-way handsh...	Wireless client sent 4/4 message of 4

10

Switch Info

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

Switch Config

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

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	00:0C:29:00:00:00	Forti-Corp-3F-PSK	802.11ax-5G	Coverage	Asymmetric Data Rates	-54 dBm
2022/05/24 13:23:42	00:0C:29:00:00:00	Forti-Corp-3F-PSK	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	00:0C:29:00:00:00	Forti-Corp-3F-PSK	802.11ac	Coverage	Asymmetric Data Rates	-58 dBm
2022/05/24 13:23:42	00:0C:29:00:00:00	Forti-Corp-3F-PSK	802.11ac	Coverage	Asymmetric Data Rates	-54 dBm

0% 5

All Clients

Client Mac Address	Channel	Radio Type	SSID	Data Rate	Bandwidth Rx	Bandwidth Tx
00:0C:29:00:00:00	60	802.11ax-5G	Forti-Corp-3F-PSK	456.00 Mbps	0	642.00 bps
00:0C:29:00:00:00	60	802.11ax-5G	Forti-Corp-3F-PSK	12.00 Mbps	0	1.77 Kbps
00:0C:29:00:00:00	60	802.11ax-5G	Forti-Corp-3F-PSK	797.20 Mbps	426.39 Kbps	45.10 Kbps

Logs

Interfering APs

Description

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

Date/Time	BSSID	Signal Strength(dBm)
2022/05/24 11:02:56	802.11ax-5G	-56
2022/05/24 11:02:56	802.11ax-5G	-52
2022/05/24 11:02:56	802.11ax-5G	-47
2022/05/24 11:02:56	802.11ax-5G	-56
2022/05/24 11:02:56	802.11ax-5G	-67
2022/05/24 11:02:56	802.11ax-5G	-56
2022/05/24 11:02:56	802.11ax-5G	-62
2022/05/24 11:02:56	802.11ax-5G	-60
2022/05/24 11:02:56	802.11ax-5G	-60
2022/05/24 11:02:56	802.11ax-5G	-65
2022/05/24 11:02:56	802.11ax-5G	-64

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

<div> <div>IMPACTED CLIENT(S)</div> <div>Show AP Details</div> <div>Search</div> </div>									
Date/Time	Client Mac Address	Device	SSID	AP Radio	Channel	Classifier	Subclassifier	Radio Type	Signal Strength
2022/05/24 14:10:42	802.11ax-5G	RJ-OnePlus	Forti-Corp-3F-PSK	2	60	Coverage hole	Distant Client	802.11ax-5G	-78
2022/05/24 14:09:42	802.11ax-5G	RJ-OnePlus	Forti-Corp-3F-PSK	2	60	Coverage hole	Distant Client	802.11ax-5G	-78
2022/05/24 10:27:55	802.11ax-5G	Forti-Corp-3F-PSK	Forti-Corp-3F-PSK	2	60	Coverage hole	Distant Client	802.11ax-5G	-77
2022/05/23 14:10:45	802.11ac	Forti-Corp-3F-PSK	CORP_83x_Tst	2	60	Coverage hole	Distant Client	802.11ac	-82

Resize Columns to Content

Reset Table

Select Columns

Date/Time

Client Mac Address

Device

SSID

AP Radio

Channel

Classifier

Subclassifier

Radio Type

Signal Strength

SNR

RSSI Neighbour AP

AP Serial

FortiGate Hostname

FortiGate Serial

Apply

Cancel

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

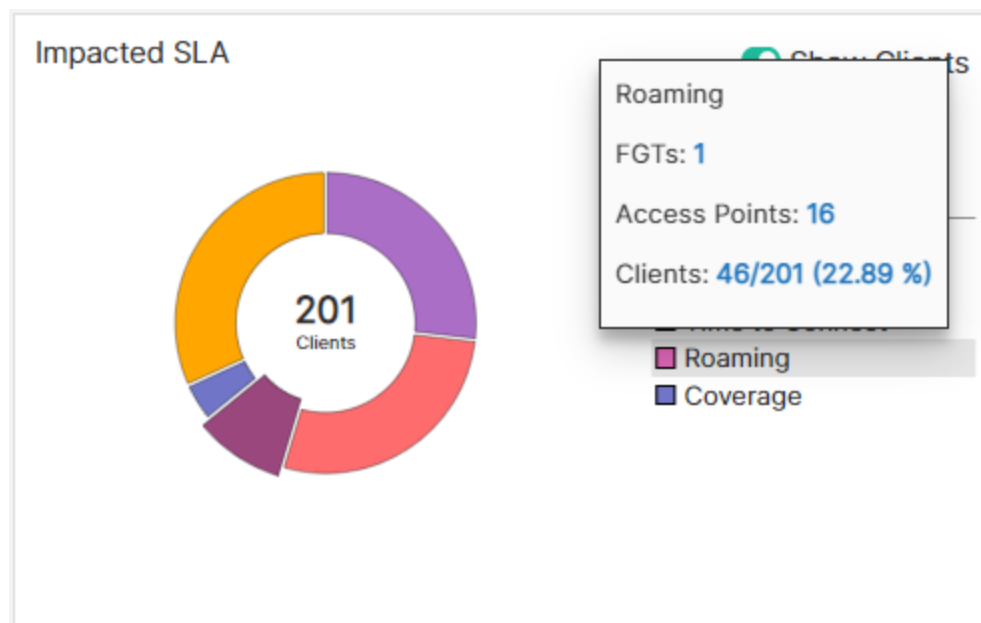
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Client MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted client is associated with.
Radio Type	The impacted radio and band information associated with the client.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Signal Strength	The signal strength of the client at the time of impact.
AP Radio	The AP radio that the client associated with.

Attribute	Description
AP Serial	The AP serial number that the client associated with.
Channel	The channel at which the client connected.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
RSSI Neighbour AP	The highest neighbour AP RSSI.
SNR	The client SNR reported at the time of impact.

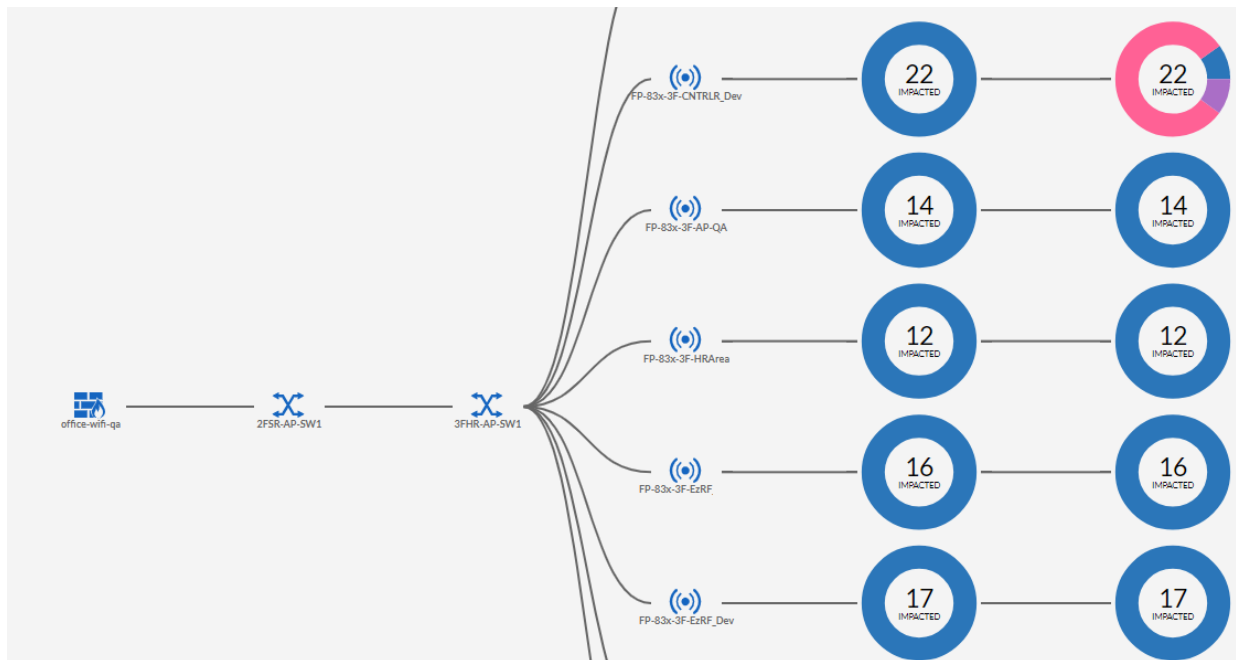
For more details on each of these tabs, see **View Logs** described earlier in the section.

Roaming

Slow roaming clients are detected based on the variation of the classifier threshold values set by the users or calculated dynamically by 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](#).



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



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

IMPACTED CLIENT(S)							
View Logs + Q Search							
Date/Time	Client Mac Address	Device	SSID	Channel	Radio	Radio Type	Classifi
43x_2F_Cafe_entry 8							
2022/07/06 12:48:44	78:14:5A:2B:3C:4D	iPhone-3	Forti-Corp-2F-PSK	11	2	802.11ax,n,g-only	11r
2022/07/06 12:21:33	78:14:5A:2B:3C:4E	iPhone-3	Forti-Corp-2F-PSK	11	2	802.11ax,n,g-only	11r
2022/07/06 12:01:11	b2:bb:5f:bd:fe:07		Forti-Corp-2F-PSK	36	1	802.11ax-5G	11r
2022/07/06 11:46:04	8a:7b:7c:7d:7e:7f	Galaxy-A21s	Forti-Corp-2F-PSK	36	1	802.11ax-5G	11r

Resize Columns to Content

Reset Table

Select Columns

✓

Date/Time

✓

Client Mac Address

✓

Device

✓

SSID

✓

Channel

✓

Radio

✓

Radio Type

✓

Classifier

✓

Sub Classifier

✓

Delay

✓

AP Serial

✓

Issue Cause

✓

Remedy

Apply

Cancel

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

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

Attribute	Description
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Delay (ms)	The delay (latency) in client roaming (milliseconds) in case of threshold breach.
Radio	The AP radio that the client associated with.
AP Serial	The AP serial number that the client associated with.
Channel	The channel at which the AP/client were operating.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.

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

Client Details ✕

[Diagnostics](#)
[AP Stats](#)
[Client Logs](#)

Issue Diagnostics

Issue Cause	<ul style="list-style-type: none"> Roaming delay observed for 11r roaming over-the-ds
Remedy	<ul style="list-style-type: none"> Review threshold computed/configured for 11r Roaming delay alerts.

Logs	Description														
Diagnostics	<p>This tab provides detailed cause of the SLA breach that impacted the client. FortiAIOps also suggests the remedy to resolve the issue.</p> <div>Issue Diagnostics</div> <table> <tr> <td>Issue Cause</td> <td> <ul style="list-style-type: none"> Roaming delay observed for 11r roaming over-the-air </td> </tr> <tr> <td>Remedy</td> <td> <ul style="list-style-type: none"> Review threshold computed/configured for 11r Roaming delay alerts. </td> </tr> </table>	Issue Cause	<ul style="list-style-type: none"> Roaming delay observed for 11r roaming over-the-air 	Remedy	<ul style="list-style-type: none"> Review threshold computed/configured for 11r Roaming delay alerts. 										
Issue Cause	<ul style="list-style-type: none"> Roaming delay observed for 11r roaming over-the-air 														
Remedy	<ul style="list-style-type: none"> Review threshold computed/configured for 11r Roaming delay alerts. 														
AP Stats	<p>This tab displays the details of the AP radio that the client associated with.</p> <div>Radio Info</div> <div> <input type="text"/> <input type="button" value="Q Search"/> </div> <table> <tr> <th>Radio Type</th><th>Bandwidth Tx</th><th>Bandwidth Rx</th><th>Channel Utilization(%)</th><th>Client Count</th><th>Oper Chan</th><th>Oper Tx Power</th></tr> <tr> <td>802.11ax-5G</td><td>209.92 Kbps</td><td>158.65 Kbps</td><td>31</td><td>15</td><td>60</td><td>10 dBm</td></tr> </table>	Radio Type	Bandwidth Tx	Bandwidth Rx	Channel Utilization(%)	Client Count	Oper Chan	Oper Tx Power	802.11ax-5G	209.92 Kbps	158.65 Kbps	31	15	60	10 dBm
Radio Type	Bandwidth Tx	Bandwidth Rx	Channel Utilization(%)	Client Count	Oper Chan	Oper Tx Power									
802.11ax-5G	209.92 Kbps	158.65 Kbps	31	15	60	10 dBm									
Client Logs	This tab provides client event logs.														

Logs

Description

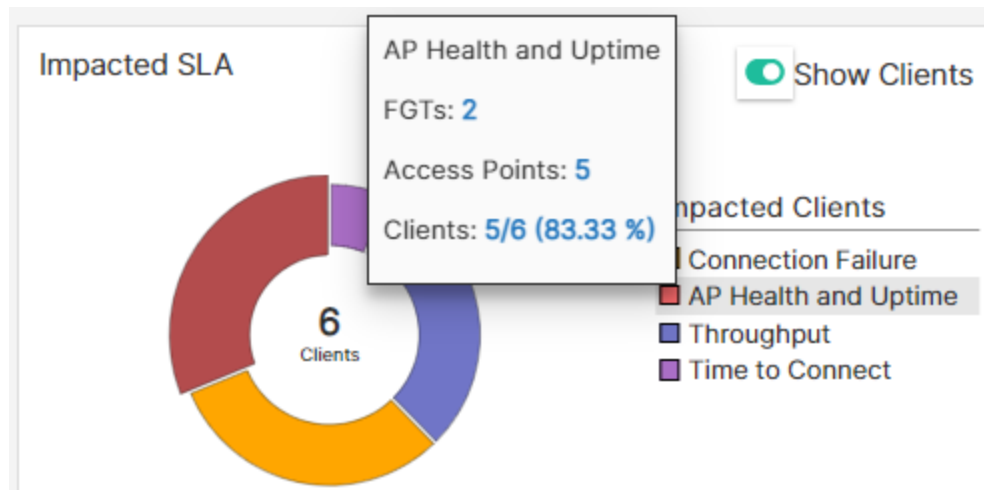
Date/Time ⌵	Level ⌵	Action ⌵	Message ⌵	Channel ⌵
2022/05/24 11:56:25	notice	client-ip-detected	Client fe:f6:7b:fe:4d:5d had an IP address detect...	60
2022/05/24 11:56:24	notice	FT-reassoc-resp	AP sent FT reassociation response frame to client...	60
2022/05/24 11:56:24	notice	FT-reassoc-req	AP received FT reassociation request frame from ...	60
2022/05/24 11:56:24	notice	FT-auth-resp	AP sent FT authentication response frame to cile...	60
2022/05/24 11:56:24	notice	FT-auth-req	AP received FT authentication request frame fro...	60
2022/05/24 11:56:11	notice	client-ip-detected	Client fe:f6:7b:fe:4d:5d had an IP address detect...	60
2022/05/24 11:56:10	notice	FT-reassoc-resp	AP sent FT reassociation response frame to client...	60
2022/05/24 11:56:10	notice	FT-reassoc-req	AP received FT reassociation request frame from ...	60
2022/05/24 11:56:10	notice	FT-auth-resp	AP sent FT authentication response frame to cile...	60
2022/05/24 11:56:10	notice	FT-auth-req	AP received FT authentication request frame fro...	60

10

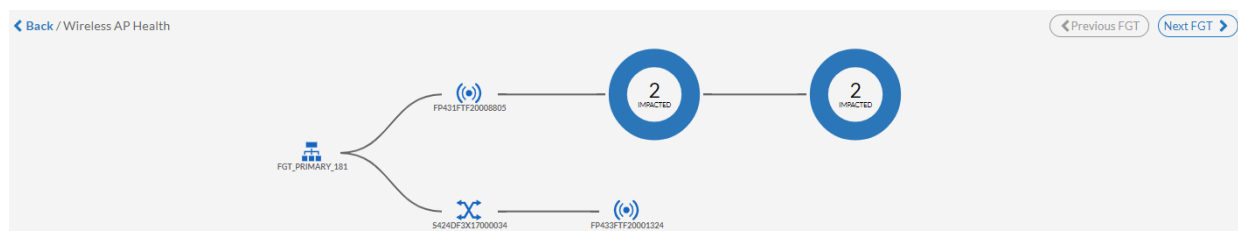
In the various throughput logs displayed, you can right-click on the table header to select the details you want to view.

AP Health and Uptime

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



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



The **AP Events** table displays issue details such as the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on.

AP EVENT(S)					
<div> <div>View Logs</div> <div> <input type="text"/> <div>Q Search</div> </div> </div>					
<div>⚙</div> Date/Time ⌵	<div>⌵</div> Switch Name ⌵	<div>⌵</div> Classifier ⌵	<div>⌵</div> Sub Classifier ⌵	<div>⌵</div> Issue Cause ⌵	<div>⌵</div> Remedy ⌵
<div> <div> <div>FP431FTF21005579</div> <div>26</div> </div> </div>					
2022/05/24 15:20:53		Memory	High Resource Utilization	<div>⚠</div> Poor FortiAP Health - High Memory [38%] usage	<div>✅</div> Rectify high interference and high
2022/05/24 15:20:51		Switch Health	FSW Poor Stats	<div>⚠</div> Poor FortiSwitch Health - Device Temperature [44.50°C] is High (...	<div>✅</div> Check and rectify if any issues w
2022/05/24 15:10:52		Switch Health	FSW Poor Stats	<div>⚠</div> Poor FortiSwitch Health - Device Temperature [44.50°C] is High (...	<div>✅</div> Check and rectify if any issues w
2022/05/24 15:10:52		Memory	High Resource Utilization	<div>⚠</div> Poor FortiAP Health - High Memory [38%] usage	<div>✅</div> Rectify high interference and high
2022/05/24 15:00:53		Memory	High Resource Utilization	<div>⚠</div> Poor FortiAP Health - High Memory [36%] usage	<div>✅</div> Rectify high interference and high

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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Switch Name	The name of the switch associated with the impacted AP/client.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
AP Serial	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
Switch Serial	The serial number of the switch associated with the impacted AP/client.

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

AP Details

Diagnostics
AP Stats
Logs
WIFI Clients
Interfering APs

Issue Diagnostics

Issue Cause	<ul style="list-style-type: none"> Poor FortiAP Health - High CPU [28%] usage
Remedy	<ul style="list-style-type: none"> 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.

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

Radio Type	Bandwidth Tx	Bandwidth Rx	Channel Utilization(%)	Client Count	Oper Chan	Oper Tx Power
802.11ax-5G	795.27 Kbps	113.15 Kbps	20	11	60	15 dBm

1

Wired Status

+ Search

Interface	Full Duplex	Link Speed(mbps)	bytes Rx	bytes Tx	Collisions	Dropped Rx	Dropped T
lan1	true	1000	442456927813	154860226111	0	762954	0

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

WIFI Clients

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

FortiAIOps 1.1.1 User Guide
Fortinet Inc.

51

Logs Description

AP Details

Impacted Clients

+ Q Search

Date/Time	Client Mac Address	Device	AP Name	Classifier	Sub Classifier
2022/07/18 15:52:32	f0:18:98:53:1f:b5	CorpWiFi-6s-MBP	FP421ETF19004722	Memory	High Resource Utilization
2022/07/18 15:52:32	f0:18:98:56:19:d4	CorpWiFi-3s-MBP	FP421ETF19004722	Memory	High Resource Utilization

2

All Clients

+ Q Search

Client Mac Address	Channel	Radio Type	SSID	Data Rate	Bandwidth Rx	Bandwidth Tx
f0:18:98:56:19:d4	6	802.11n	24ghz-25bridge	136.00 Mbps	0	0
f0:18:98:53:1f:b5	6	802.11n	24ghz-25bridge	169.00 Mbps	0	0

OK Cancel

Interfering APs

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

Date/Time	BSSID	Signal Strength(dBm)
2022/05/24 11:02:56	80:18:98:53:1f:b5	-56
2022/05/24 11:02:56	80:18:98:53:1f:b5	-52
2022/05/24 11:02:56	80:18:98:53:1f:b5	-47
2022/05/24 11:02:56	80:18:98:53:1f:b5	-56
2022/05/24 11:02:56	80:18:98:53:1f:b5	-67
2022/05/24 11:02:56	80:18:98:53:1f:b5	-56
2022/05/24 11:02:56	80:18:98:53:1f:b5	-62
2022/05/24 11:02:56	80:18:98:53:1f:b5	-60
2022/05/24 11:02:56	80:18:98:53:1f:b5	-60
2022/05/24 11:02:56	80:18:98:53:1f:b5	-65
2022/05/24 11:02:56	80:18:98:53:1f:b5	-64

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

IMPACTED CLIENT(S)

Show AP Details + Q Search

Date/Time	Client Mac Address	Device	Classifier
FP431TF20010590 713			
2022/07/06 10:48:49	80:18:98:53:1f:b5	merus-MBP	Memory
2022/07/06 10:48:49	80:18:98:53:1f:b5	meru111s-MBP-2	Memory
2022/07/06 10:48:49	80:18:98:53:1f:b5	meru105s-MBP	Memory
2022/07/06 10:38:49	80:18:98:53:1f:b5	merus-MBP	Memory
2022/07/06 10:38:49	80:18:98:53:1f:b5	meru105s-MBP	Memory

Resize Columns to Content
 Reset Table
 Select Columns

- ✓ Date/Time
- ✓ Client Mac Address
- ✓ Device
- ✓ Classifier
- ✓ Sub Classifier
- AP IP Address
- AP Serial
- FortiGate Hostname
- FortiGate Serial
- Radio
- Sequence Number
- SSID

Apply Cancel

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

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

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

AP Details ×

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

Issue Diagnostics	
Issue Cause	<ul style="list-style-type: none"> Poor FortiAP Health - High CPU [28%] usage
Remedy	<ul style="list-style-type: none"> 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	<p>This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue.</p> <table border="1"> <thead> <tr> <th colspan="2">Issue Diagnostics</th> </tr> </thead> <tbody> <tr> <td>Issue Cause</td> <td> <ul style="list-style-type: none"> Poor FortiAP Health - High CPU [28%] usage </td> </tr> <tr> <td>Remedy</td> <td> <ul style="list-style-type: none"> Rectify high interference and high client density issues, if any, and also check if any resource intensive features are enabled. Also, check if there's STP loop in the network. </td> </tr> </tbody> </table>	Issue Diagnostics		Issue Cause	<ul style="list-style-type: none"> Poor FortiAP Health - High CPU [28%] usage 	Remedy	<ul style="list-style-type: none"> 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.
Issue Diagnostics							
Issue Cause	<ul style="list-style-type: none"> Poor FortiAP Health - High CPU [28%] usage 						
Remedy	<ul style="list-style-type: none"> 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.						

Logs

Description

Radio Info

 Search

Radio Type	Bandwidth Tx	Bandwidth Rx	Channel Utilization(%)	Client Count	Oper Chan	Oper Tx Power
802.11ax-5G	795.27 Kbps	113.15 Kbps	20	11	60	15 dBm

Wired Status

 Search

Interface	Full Duplex	Link Speed(mbps)	bytes Rx	bytes Tx	Collisions	Dropped Rx	Dropped Tx
lan1	true	1000	442456927813	154860226111	0	762954	0

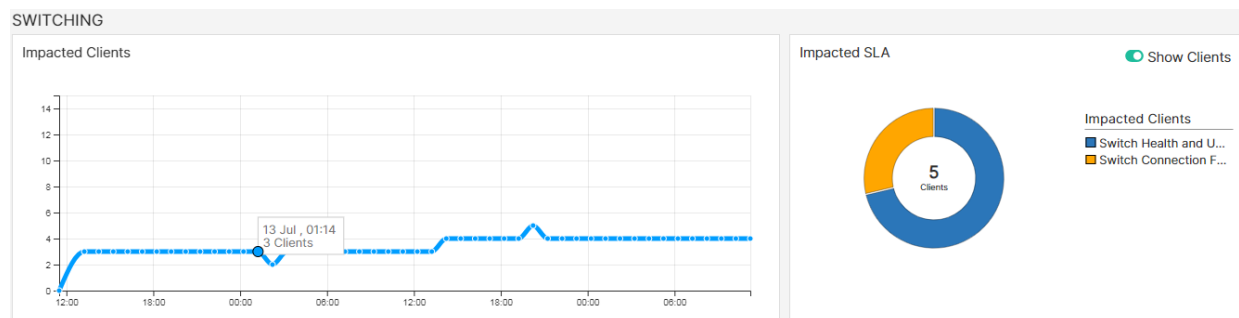
Interfering APs

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

Date/Time	BSSID	Signal Strength(dBm)
2022/05/24 11:02:56	802.11ax-5G	-56
2022/05/24 11:02:56	802.11ax-5G	-52
2022/05/24 11:02:56	802.11ax-5G	-47
2022/05/24 11:02:56	802.11ax-5G	-56
2022/05/24 11:02:56	802.11ax-5G	-67
2022/05/24 11:02:56	802.11ax-5G	-56
2022/05/24 11:02:56	802.11ax-5G	-62
2022/05/24 11:02:56	802.11ax-5G	-60
2022/05/24 11:02:56	802.11ax-5G	-60
2022/05/24 11:02:56	802.11ax-5G	-65
2022/05/24 11:02:56	802.11ax-5G	-64

Switching

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



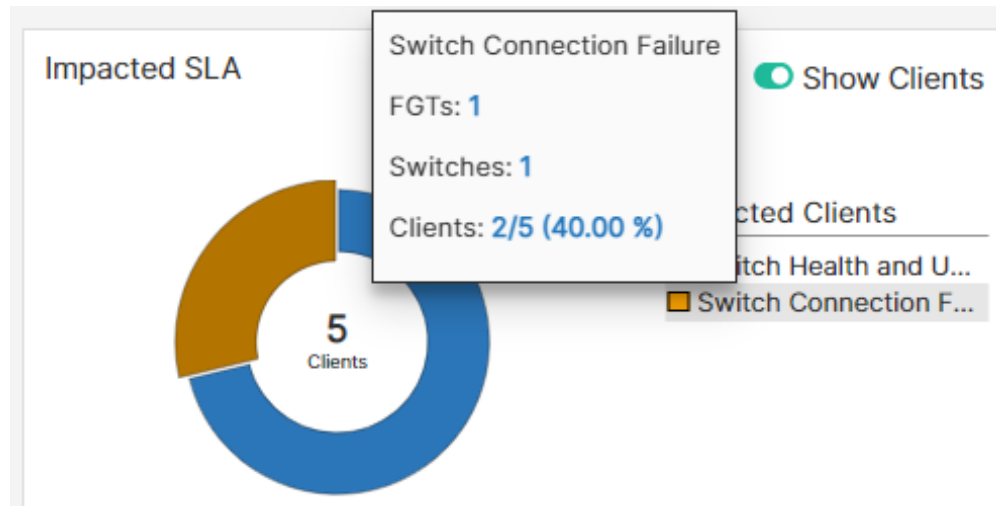
SLAs, Topology and Logs

The following SLAs are detected and reported by 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. In each impacted SLA panel, you can select **Show Clients** to view the impacted client count or click **Show Switches** to view the impacted switch count.

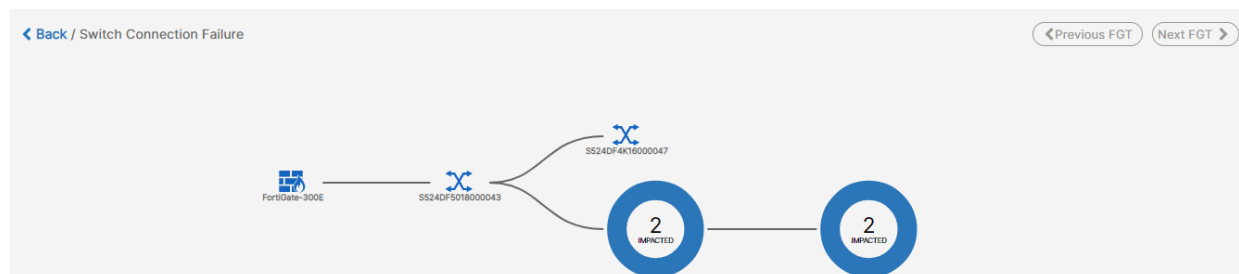
- [Switch Connection Failure](#)
- [Switch Health and Uptime](#)

Switch Connection Failure

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



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



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

SWITCHES						
View Logs + Search						
Date/Time	Switch Name	Client Mac Address	Device	Classifier	Sub Classifier	
2022/07/13 16:55:40	SS24DF5018000043	SS24DF4K16000047	SS24DF4K16000047	MAC Limit Exceed	Port MAC Limit Exceed	Interface N
2022/07/13 16:51:31	SS24DF5018000043	SS24DF4K16000047	SS24DF4K16000047	MAC Limit Exceed	Port MAC Limit Exceed	Interface N
2022/07/13 16:49:06	SS24DF5018000043	SS24DF4K16000047	SS24DF4K16000047	MAC Limit Exceed	Port MAC Limit Exceed	Interface N
2022/07/13 16:47:04	SS24DF5018000043	SS24DF4K16000047	SS24DF4K16000047	MAC Limit Exceed	Port MAC Limit Exceed	Interface N
2022/07/13 16:45:31	SS24DF5018000043	SS24DF4K16000047	SS24DF4K16000047	MAC Limit Exceed	Port MAC Limit Exceed	Interface N

Resize Columns to Content
 Reset Table
Select Columns
☒ Date/Time
☒ Switch Name
☒ Client Mac Address
☒ Device
☒ Classifier
☒ Sub Classifier
☒ Issue Cause
☒ Remedy
☐ FortiGate Hostname
☐ FortiGate Serial
☐ Sequence Number
☐ Switch Serial

Apply Cancel

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

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

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

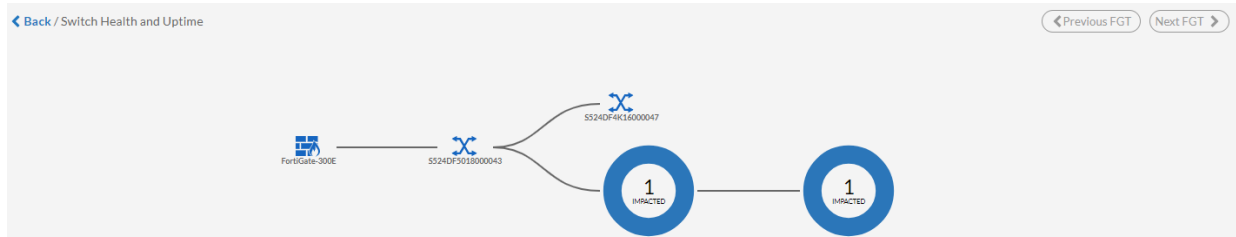
Switch Logs	
Diagnostics	Logs
Issue Diagnostics	
Issue Cause	<ul style="list-style-type: none"> Interface MAC learning limit exceeded on port7 Packet VID 100
Remedy	<ul style="list-style-type: none"> Review the MAC learning limit configured for the port7

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		
<input type="text" value="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	

Switch Health and Uptime

Displays the switch health based on the configured switch health threshold values and the status of the switch (Up/Down). The associated impacted FortiGate controller, switch, and client count are displayed in a collapsible topology.



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

SWITCHES						
View Logs 🔍 Search						
Date/Time	Switch Name	Client Mac Address	Device	Classifier	Sub Classifier	Issue Cause
2022/05/24 12:30:51	S524DF501800043	08:00:27:00:00:00	S524DF501800043	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF501800043
2022/05/24 12:20:52	S524DF501800043	08:00:27:00:00:00	S524DF501800043	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF501800043
2022/05/24 12:10:51	S524DF501800043	08:00:27:00:00:00	S524DF501800043	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF501800043
2022/05/24 12:00:51	S524DF501800043	08:00:27:00:00:00	S524DF501800043	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF501800043
2022/05/24 11:50:51	S524DF501800043	08:00:27:00:00:00	S524DF501800043	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF501800043

Resize Columns to Content
 Reset Table
 Select Columns

☒ Date/Time
☒ Switch Name
☒ Client Mac Address
☒ Device
☒ Classifier
☒ Sub Classifier
☒ Issue Cause
☒ Remedy
☐ FGT Serial
☐ FortiGate Hostname
☐ Sequence Number
☐ Switch Serial

Apply Cancel

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

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

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

Switch Logs ×

[Diagnostics](#)
[Logs](#)

Issue Diagnostics

Issue Cause	<ul style="list-style-type: none"> High CPU usage [40%] on switch
Remedy	<ul style="list-style-type: none"> 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.

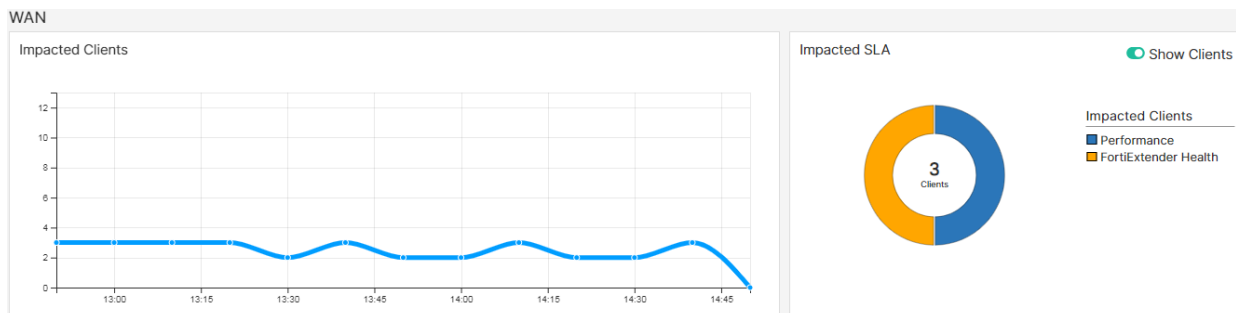
Switch Logs

[Diagnostics](#)
[Logs](#)

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

WAN

The WAN panel displays the Impacted Clients information for Performance SLA and FortiExtenders failures. Any client that breaches the configured SLA thresholds are reported. In each SLA panel, you can select **Show Clients** to view the impacted client count or click **Show Interfaces** to view the impacted interface count.



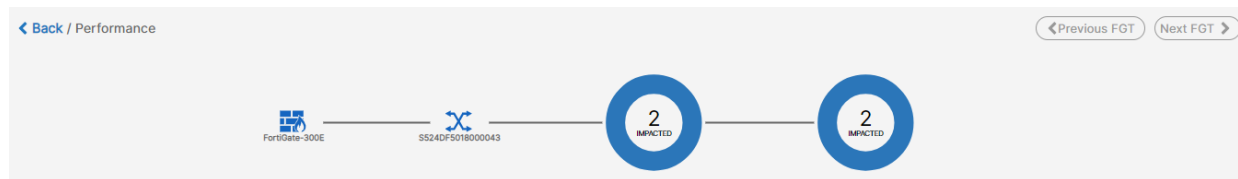
SLAs, Topology and Logs

The following SLAs are detected and reported by FortiAIOps for WAN.

- Performance
- FortiExtender Health

Performance

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



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

The screenshot shows the 'IMPACTED CLIENT(S)' table with columns: Date/Time, AP Name, Switch Name, Client Mac Address, Device, Health Check, and Source Interface. A dropdown menu is open, showing a list of columns to select. The table contains four rows of data, with the first row highlighted in blue.

Date/Time	AP Name	Switch Name	Client Mac Address	Device	Health Check	Source Interface
2022/07/06 13:02:10					google_dns	internal
2022/07/06 13:02:10					google_dns	internal
2022/07/06 13:02:10					google_dns	internal
2022/07/06 12:59:10					google_dns	internal

Select Columns

- ☒ Date/Time
- ☒ AP Name
- ☒ Switch Name
- ☒ Client Mac Address
- ☒ Device
- ☒ Health Check
- ☒ Source Interface
- ☒ Classifier
- ☒ Subclassifier
- ☒ Jitter
- ☒ Packet Loss(%)
- ☒ Latency
- ☒ Breach Summary
- ☒ Issue Cause
- ☒ Remedy
- ☒ Client Type
- ☐ AP Serial
- ☐ FortiGate Hostname
- ☐ FortiGate Serial
- ☐ Switch Serial

Buttons: Apply, Cancel

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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiGate Serial	The serial number of the associated FortiGate.
AP Serial	The serial number of the associated AP.
Client MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
Issue Cause	The detailed cause of the SLA breach that impacted the client/AP/FortiGate/FortiExtender.
Remedy	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Health Check	The performance SLA check configured in FortiGate.
Source Interface	The source interface name.

Attribute	Description
Jitter(ms)	The amount of jitter (milliseconds) reported for the client.
Packet Loss(%)	The percentage of packet loss reported for the client.
Latency(ms)	The amount of latency (milliseconds) reported for the client.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
Breach Summary	The WAN SLA threshold that was breached.
Client Type	The client type that is impacted, wireless or wired.

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

Client Details ×							
CLIENT LOGS							
<input type="text"/>							
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

FortiExtender Health

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



The following image displays the SIM, device failures and Impacted clients for FortiExtender health SLAs.

						<div> <div>Best Fit Columns</div> <div>Reset Table</div> <div>Select Columns</div> <div> <div>✓ Date/Time</div> <div>✓ Client Mac Address</div> <div>✓ Device</div> <div>✓ Classifier</div> <div>✓ Subclassifier</div> <div>✓ Issue Cause</div> <div>✓ Remedy</div> <div>✓ Client Type</div> <div>AP Name</div> <div>AP Serial</div> <div>Destination Interface</div> <div>FortiExtender Name</div> <div>FortiExtender Serial</div> <div>FortiGate Hostname</div> <div>FortiGate Serial</div> <div>Source Interface</div> <div>Switch Name</div> <div>Switch Serial</div> </div> <div> <div>Apply</div> <div>Cancel</div> </div> </div>
FORTIEXTENDER FAILURES						
View Logs Search						
Date/Time	Client Mac Address	Device	Classifier	Subclassifier	Issue Cause	
2022/12/02 16:17:25	88:0d:00:00:00:00	88:0d:00:00:00:00	SIM Failure	SIM Inactive or Not Found	SIM at slot 2 on FortiExtender FX2	
2022/12/02 16:17:25	88:0d:00:00:00:00	88:0d:00:00:00:00	SIM Failure	SIM Inactive or Not Found	SIM at slot 2 on FortiExtender FX2	
2022/12/02 16:17:25	88:0d:00:00:00:00	88:0d:00:00:00:00	SIM Failure	SIM Inactive or Not Found	SIM at slot 2 on FortiExtender FX2	
2022/12/02 16:17:13	88:0d:00:00:00:00	88:0d:00:00:00:00	Carrier Failure	Carrier Disconnect	Carrier Jio 4G at SIM slot 2 on FortiExtender FX2	

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

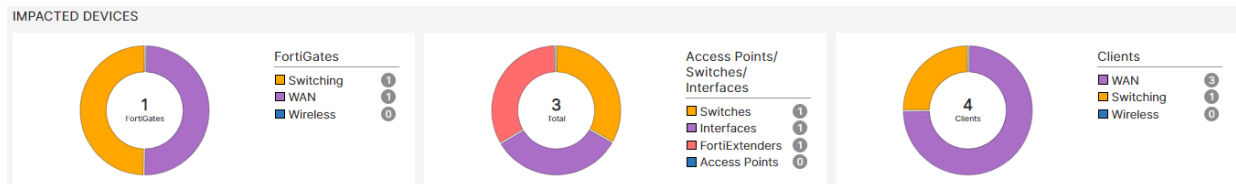
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiGate Serial	The serial number of the associated FortiGate.
AP Serial	The serial number of the associated AP.
AP Name	The name of the associated AP.
Client MAC Address	The MAC address of the impacted client device.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

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

Extender Logs ✕	
Diagnostics	
Issue Diagnostics	
Issue Cause	<ul style="list-style-type: none"> Device temperature high [69.60°C] on FortiExtender FX201E5920012136 detected
Remedy	<ul style="list-style-type: none"> Please ensure FortiExtender is placed in a space with sufficient air circulation and there are no other external source nearby that could cause FortiExtender to overheat

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 **Monitor > Impacted Devices**.




- [FortiGates](#)
- [Access Points/ Switches/ Interfaces/FortiExtenders](#)
- [Clients](#)

FortiGates

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


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

FORTIGATES - WIRELESS SLA					
View in Topology  Search					
FortiGate	FortiGate IP Address	Impacted APs	Impacted Clients	Impacted SLAs	
FGT60ETK1					<div> <div>AP Health and Uptime</div> <div>Connection Failure</div> <div>Throughput</div> <div>Time to Connect</div> </div>
FGT60ETK1		2	3		<div> <div>AP Health and Uptime</div> <div>Connection Failure</div> <div>Throughput</div> <div>Time to Connect</div> </div>
FortiGate-101F					
FG101		1	3		<div> <div>Throughput</div> <div>AP Health and Uptime</div> <div>Connection Failure</div> </div>

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

FORTIGATES - WAN SLA								
View in Topology  Search								
HostName	FortiGate Serial	FortiGate IP Address	Impacted APs	Impacted Switches	Impacted Interfaces	Impacted Clients	Extenders	Impacted SLAs
FortiGate-300E	FG3H	10.10.10.10	0	1	1	3	1	<div> <div>Pe</div> <div>Fo</div> </div>


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

FORTIGATES - SWITCHING SLA						
View in Topology  Search						
HostName	Serial	IP Address	Impacted Switches	Impacted Clients	Impacted SLAs	
FortiGate-300E	FG3H	10.10.10.10	1	1		<div> <div>Switch Health and Uptime</div> </div>


Access Points/ Switches/ Interfaces/FortiExtenders

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


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

ACCESS POINTS						
View in Topology  Search						
AP Name	AP Serial	AP IP Address	FortiGate HostName	Impacted Clients	Impacted SLAs	
FG101FTK						<div> <div>AP Health and Uptime</div> <div>Connection Failure</div> <div>Time to Connect</div> <div>Throughput</div> </div>
FGT60ETK1						
FGT60ETK1			FGT60ETK19099SX7	3		<div> <div>AP Health and Uptime</div> <div>Connection Failure</div> <div>Time to Connect</div> <div>Throughput</div> </div>
FGT60ETK1			FGT60ETK19099SX7	2		<div> <div>Time to Connect</div> <div>Connection Failure</div> </div>


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

INTERFACES			
View in Topology  Search			
FortiGate HostName	Interface	Impacted Clients	Impacted SLAs
office-wifi-qa	exit-int-1	76	Performance
office-wifi-qa	exit-int-2	75	Performance

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

SWITCHES				
View in Topology  Search				
Switch Hostname	Switch IP	FortiGate HostName	Impacted Clients	Impacted SLAs
10.10.10.10	10.10.10.10	FortiGate-300E	1	Switch Health and Uptime


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

FORTIEXTENDERS				
View in Topology  Search				
FortiGate HostName	FortiExtender Name	Interface	Impacted Clients	Impacted SLAs
FortiGate-300E	QA-Extender		3	FortiExtender Health

Clients

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

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

WIRELESS CLIENTS				
View in Topology  Search				
Client	FortiGate Hostname	AP Name	Impacted SLAs	
FP431TF20			Connection Failure	
6			Time to Connect	
			Throughput	
			AP Health and Uptime	
			Connection Failure	
			Time to Connect	
			Throughput	
			AP Health and Uptime	

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

WAN CLIENTS				
View in Topology + Q Search				
Client Mac Address	FortiGate Hostname	AP Name	Switch Name	Impacted SLAs
FEXWAN1 7				
...	FortiGate-300E			Performance FortiExtender Health
...	FortiGate-300E			Performance FortiExtender Health
...	FortiGate-300E			Performance FortiExtender Health
...	FortiGate-300E			Performance

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

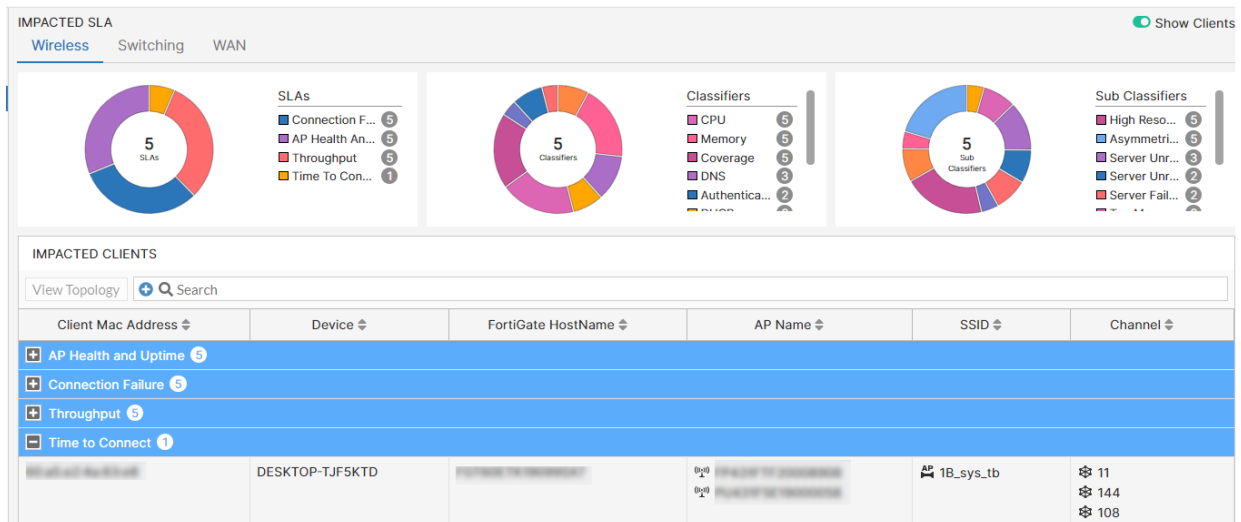
SWITCHING CLIENTS				
View in Topology + Q Search				
Client Mac Address	FortiGate Serial	FortiGate Hostname	Switch Name	Impacted SLAs
S524DF5018000043 1				
...	...	FortiGate-300E	...	Switch Health and Uptime

Impacted SLA

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

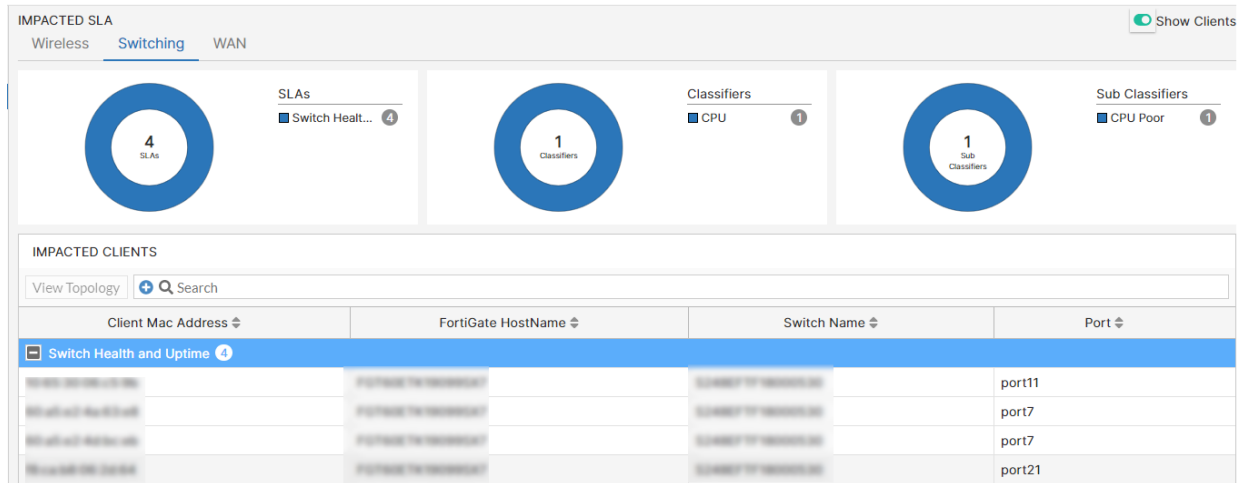
Wireless

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



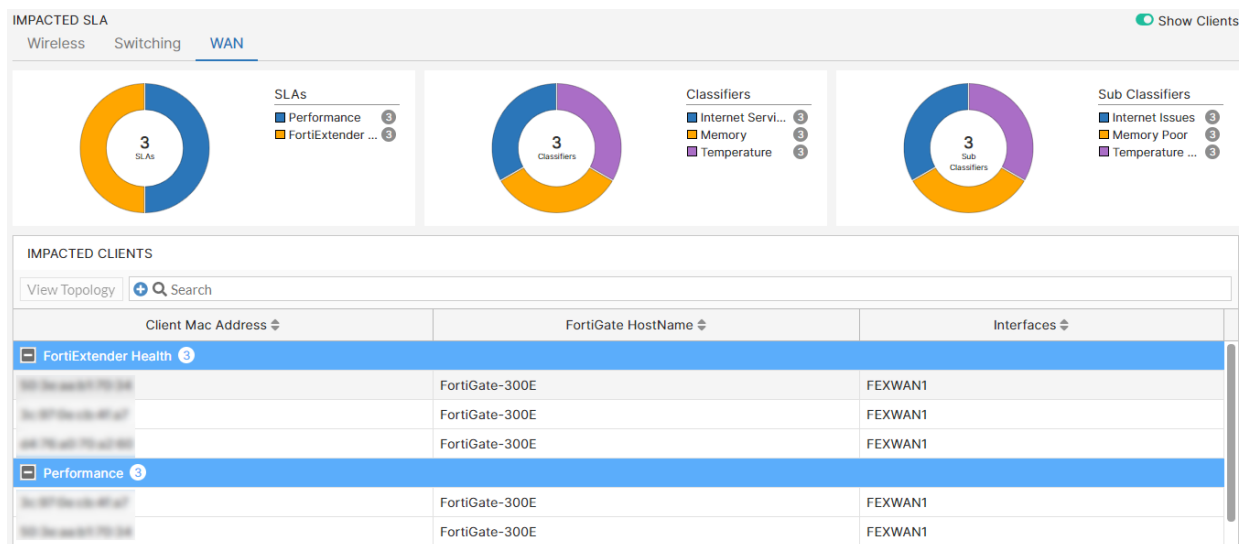
Switching

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



WAN

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



Select any device listed in the **Impacted Devices** table and click on **View Topology** for topology and other details. For details on the SLAs, topology, and logs, see section [Overview](#).

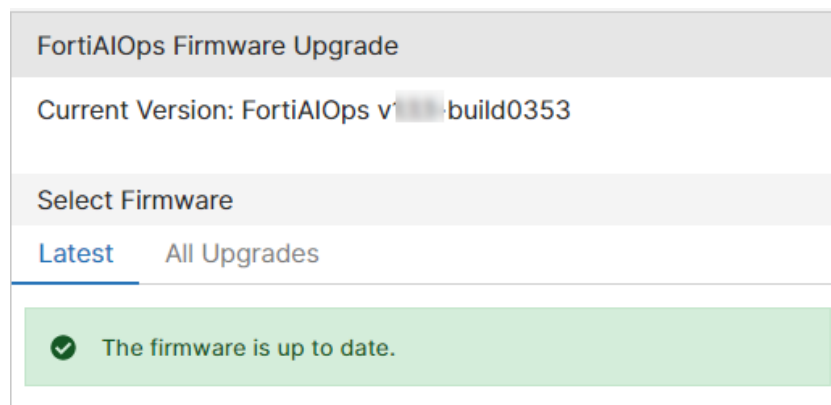
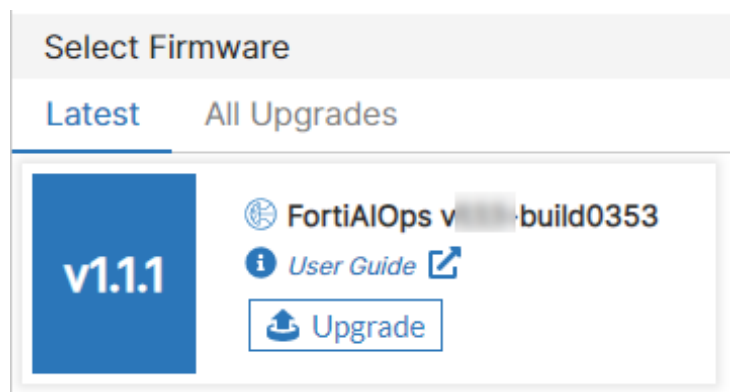
Administration

This section describes steps to upgrade firmware and download diagnostics information.

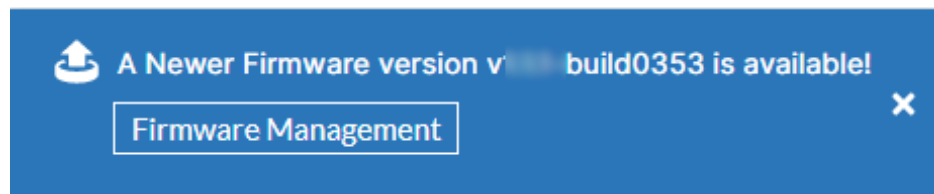
- [Upgrading Firmware](#)
- [Diagnostics](#)

Upgrading Firmware

You can upgrade to the latest FortiAIOPS firmware version in **Administration > Firmware Upgrade**. Select the latest available firmware version in the **Latest** tab and click **Upgrade**. The **All Upgrades** tab displays multiple upgrade versions (if available), you can select and upgrade to the relevant one..



When you login into FortiAIOPS with an older firmware version, you are prompted for an upgrade. Click on **Firmware Management** for upgrading.

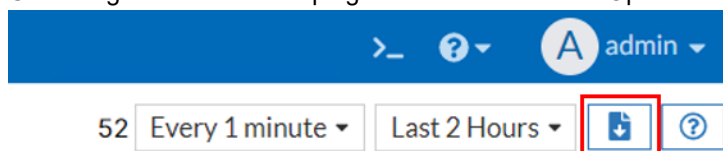


Note: FortiAI Ops reboots after successful firmware upgrade.

Diagnostics

You can collect the FortiAI Ops diagnostics comprising of system, application and process logs from the dashboard page, download them to a local folder and send to *Fortinet Support* to aid in troubleshooting.

1. Click Diagnostics icon on top right corner of the FortiAI Ops overview page.



2. Select the required diagnostics. Three diagnostics options are available:

- a. system
- b. application
- c. aiops

Diagnostics

Diagnostics Options are ☐ system
☐ application
☐ aiops


3. Click **Create File** to generate the diagnostics data.
4. Click **Download Latest File** to download the diagnostics data to the local folder.

Special Notes

The following are applicable in this release of FortiAI Ops.

- FortiAI Ops data backup and restore is not supported.
- Enable application control in the firewall policy to generate forward traffic.
- WAN clients are identified from forward traffic.

www.fortinet.com



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.