FortiAIOps - User Guide

Version 1.0.1

October 12, 2021
FortiAIOps 1.0.1 User Guide

TABLE OF CONTENTS

Change log

Date	Change description
2021-10-12	FortiAIOps 1.0.1 release version.

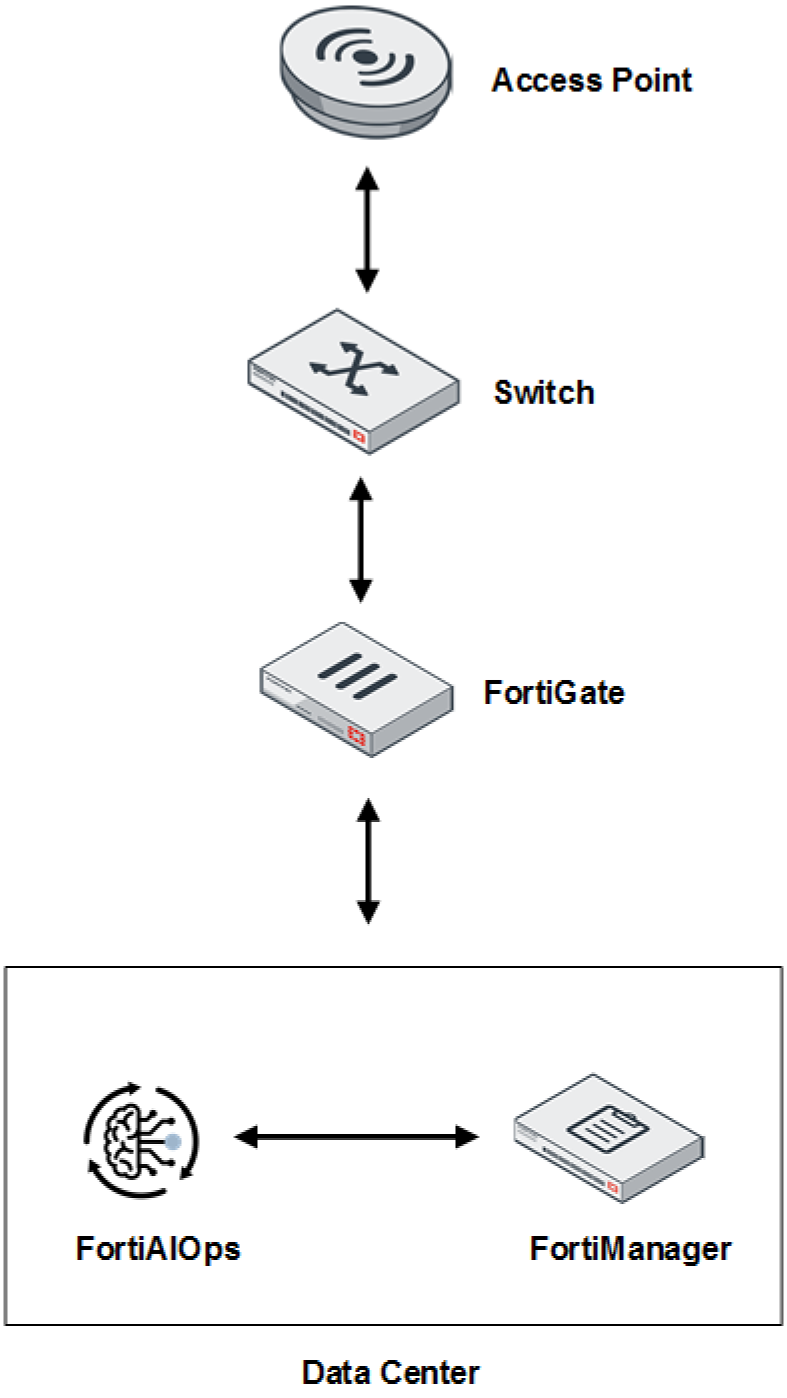
Overview

FortiAIOps 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. FortiAIOps 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.

FortiAIOps 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 FortiAIOps user interface that supports screen size of 1024x768, 1280x800, 1366x768, 1920x1080, and also mobile devices' screens.

The FortiAIOps tool provides the following advantages.

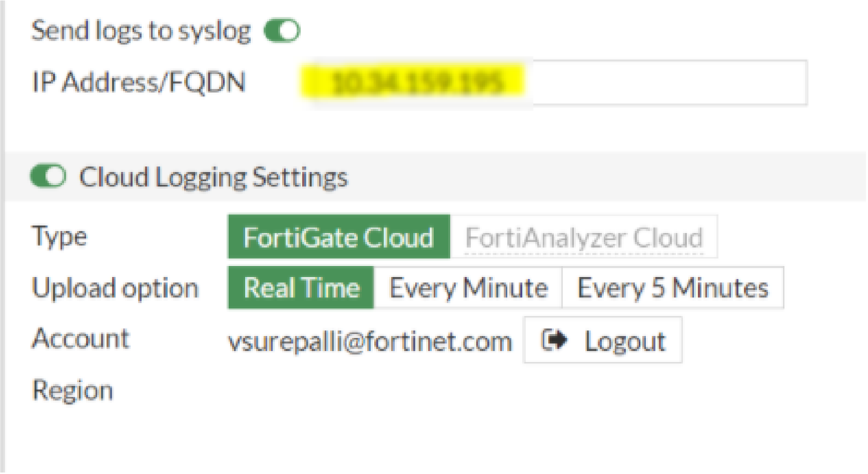
- Maximizes the uptime of your organization's network infrastructure.
- Reduces the time taken to diagnose network issues, thereby the response time.
- Increases the productivity of network users and that of your organization.



The FortiAIOps 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.

FortiAIOps 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.



Send logs to syslog ●

IP Address/FQDN [redacted]

● Cloud Logging Settings

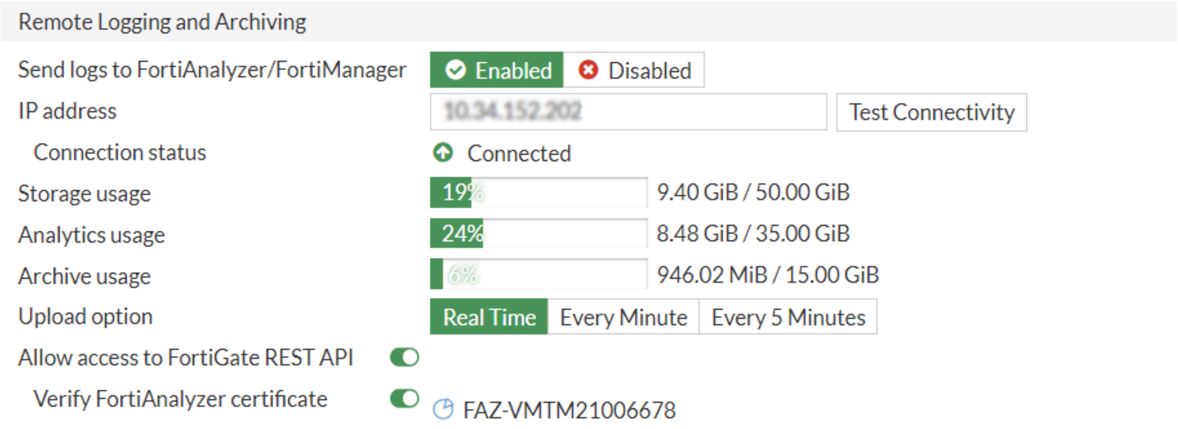
Type [✓ FortiGate Cloud] FortiAnalyzer Cloud

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

Account vsurepalli@fortinet.com Logout

Region

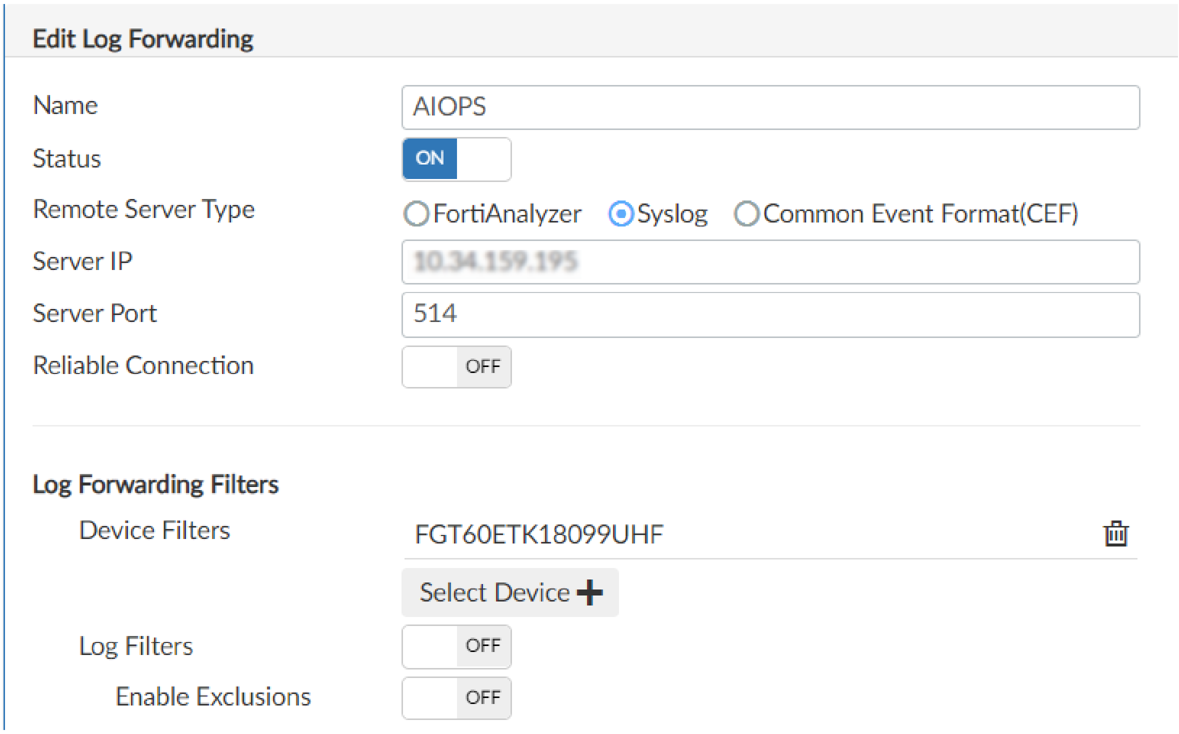
- FortiAnalyzer log forwarding - Navigate to **Log Settings** in the FortiGate GUI and enable FortiAnalyzer log forwarding.



Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager	[✓ Enabled] Disabled
IP address	[redacted] Test Connectivity
Connection status	Connected
Storage usage	19% 9.40 GiB / 50.00 GiB
Analytics usage	24% 8.48 GiB / 35.00 GiB
Archive usage	6% 946.02 MiB / 15.00 GiB
Upload option	[✓ Real Time] Every Minute Every 5 Minutes
Allow access to FortiGate REST API	●
Verify FortiAnalyzer certificate	● FAZ-VMTM21006678

Navigate to **Log Forwarding** in the FortiAnalyzer GUI, specify the FortiManager **Server Address** and select the FortiGate controller in **Device Filters**.



Edit Log Forwarding

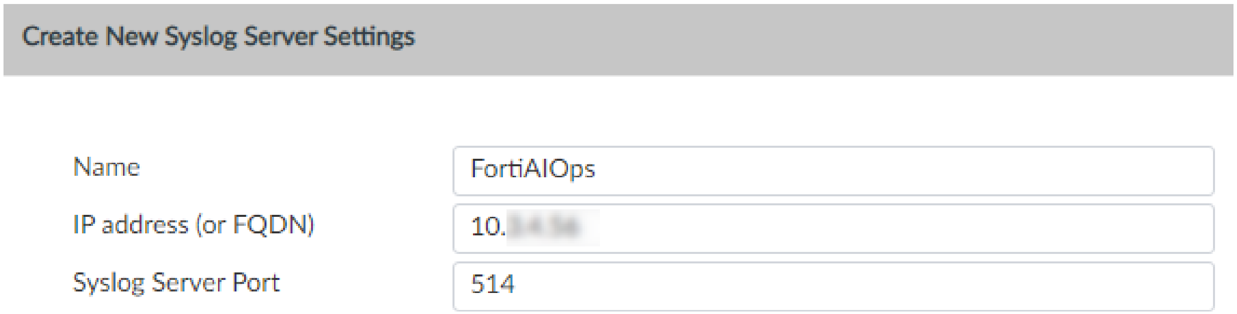
Name	AIOPS
Status	ON
Remote Server Type	○ FortiAnalyzer ● Syslog ○ Common Event Format(CEF)
Server IP	[redacted]
Server Port	514
Reliable Connection	OFF

Log Forwarding Filters

Device Filters	FGT60ETK18099UHF
	Select Device ➕
Log Filters	OFF
Enable Exclusions	OFF

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

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, and the port.



Create New Syslog Server Settings

Name	FortiAIOps
IP address (or FQDN)	10.[redacted]
Syslog Server Port	514

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*.

Getting Started

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

ADOM and Non-ADOM Modes

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

Notes:

- While creating an ADOM, select FortiGate version 6.4 or 7.0 to enable access to FortiAIOps.
- In the ADOM mode, you can add FortiGate controllers managed by the particular ADOM of the FortiManager. FortiAIOps 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 FortiAIOps, 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.

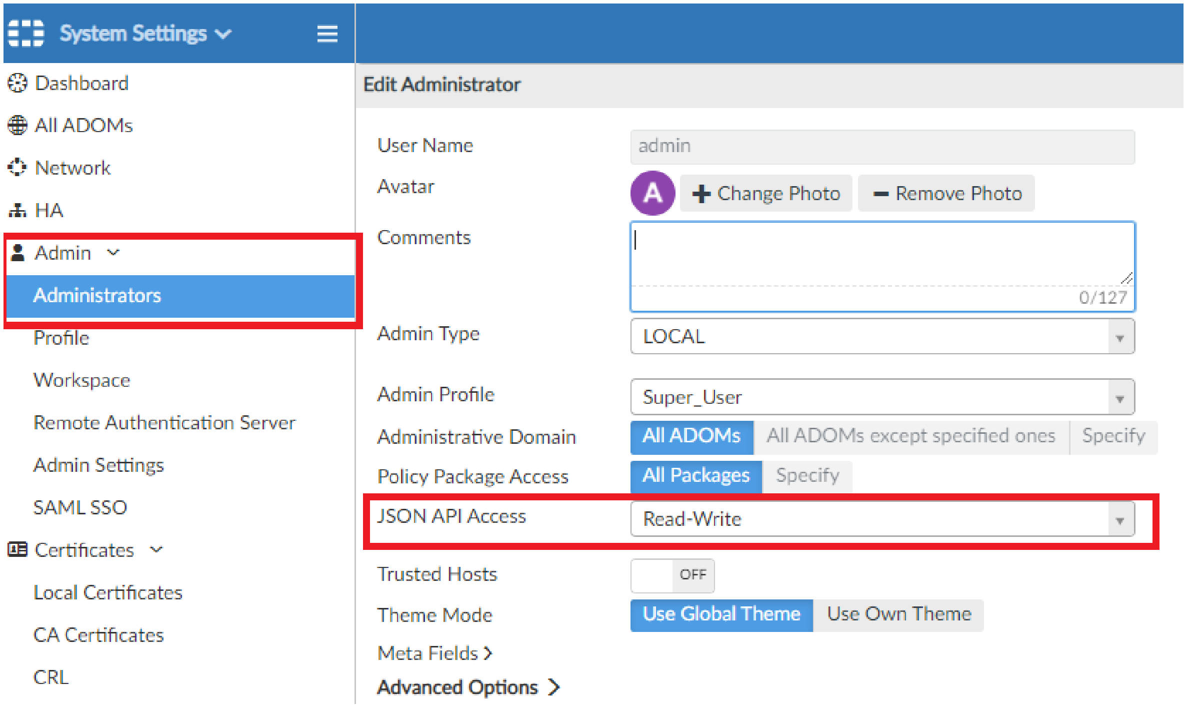
1. Delete all non-root ADOMs.
   Only after removing all the non-root ADOMs can ADOMs be disabled.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, toggle the *Administrative Domain* switch to *OFF*.
   You will be automatically logged out of the FortiManager and returned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

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

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.



Edit Administrator

User Name: admin
Avatar: A
Comments: 0/127
Admin Type: LOCAL
Admin Profile: Super_User
Administrative Domain: [✓ All ADOMs] All ADOMs except specified ones Specify
Policy Package Access: [✓ All Packages] Specify
JSON API Access: Read-Write
Trusted Hosts: OFF
Theme Mode: [✓ Use Global Theme] Use Own Theme

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 on page 11
- Adding and Managing FortiGate Controllers on page 11

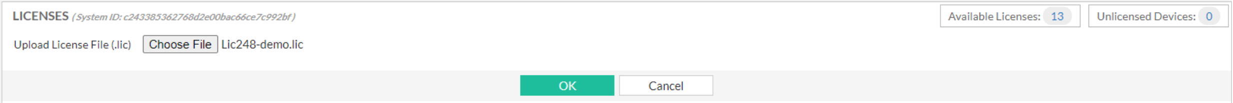
Licensing

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.

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.

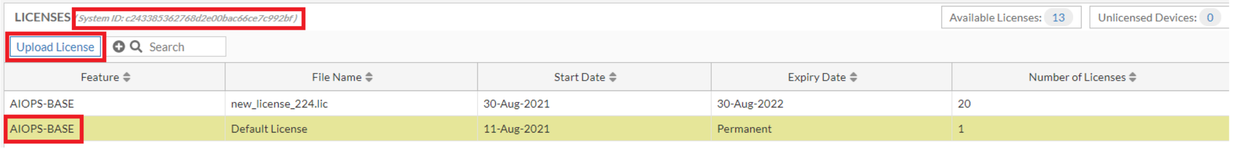


LICENSES *(System ID: c243385362768d2e00bac66ce7c992bf)*

Available Licenses: 13 | Unlicensed Devices: 0

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

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

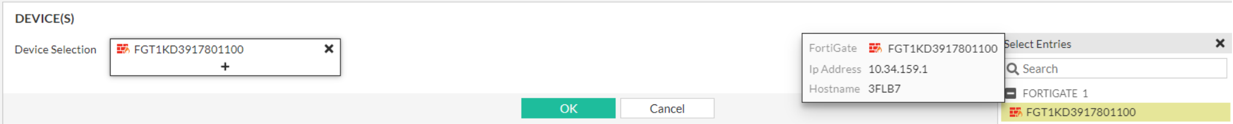
Feature	File Name	Start Date	Expiry Date	Number of Licenses
AIOPS-BASE	new_license_224.lic	30-Aug-2021	30-Aug-2022	20
AIOPS-BASE	Default License	11-Aug-2021	Permanent	1

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 9. 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.

Click **Add** and select the FortiGate controllers in **Device Selection**.



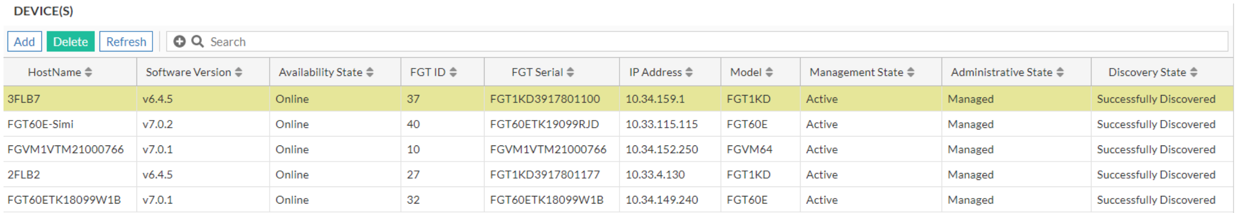
DEVICE(S)

Device Selection: FGT1KD3917801100

FortiGate: FGT1KD3917801100
Ip Address: 10.34.159.1
Hostname: 3FLB7

The added FortiGate controller is now listed.

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



DEVICE(S)

HostName	Software Version	Availability State	FGT ID	FGT Serial	IP Address	Model	Management State	Administrative State	Discovery State
3FLB7	v6.4.5	Online	37	FGT1KD3917801100	10.34.159.1	FGT1KD	Active	Managed	Successfully Discovered
FGT60E-Simi	v7.0.2	Online	40	FGT60ETK19099RJD	10.33.115.115	FGT60E	Active	Managed	Successfully Discovered
FGVM1VTM21000766	v7.0.1	Online	10	FGVM1VTM21000766	10.34.152.250	FGVM64	Active	Managed	Successfully Discovered
2FLB2	v6.4.5	Online	27	FGT1KD3917801177	10.33.4.130	FGT1KD	Active	Managed	Successfully Discovered
FGT60ETK18099W1B	v7.0.1	Online	32	FGT60ETK18099W1B	10.34.149.240	FGT60E	Active	Managed	Successfully Discovered

SLA Configurations

This section explains how to configure Service Level Agreement (SLA) to define values to match network deployment and required thresholds.

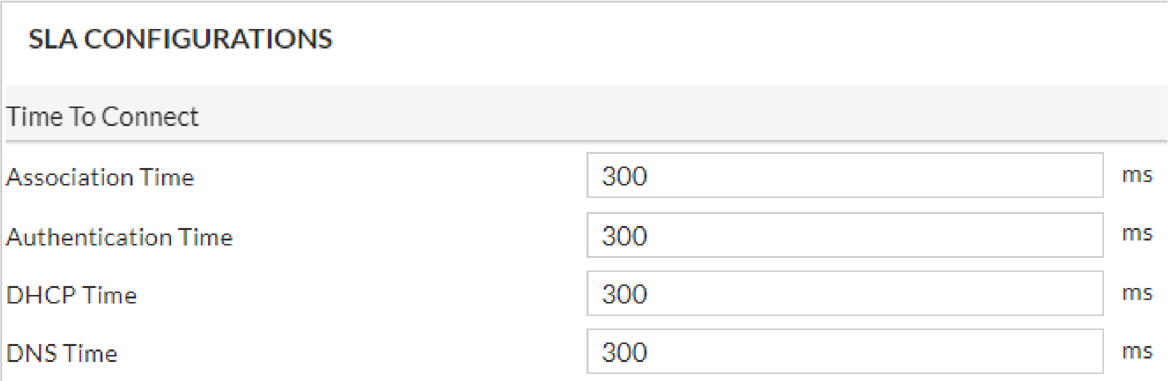
- Time To Connect on page 13
- AP Health and Switch Health on page 13

Time To Connect

These configurations compute the time taken by devices to connect to the network. Based on the configured thresholds, statistics are displayed in the Monitor on page 15 tab.

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

- **Association** - The time taken 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.



SLA CONFIGURATIONS

Time To Connect

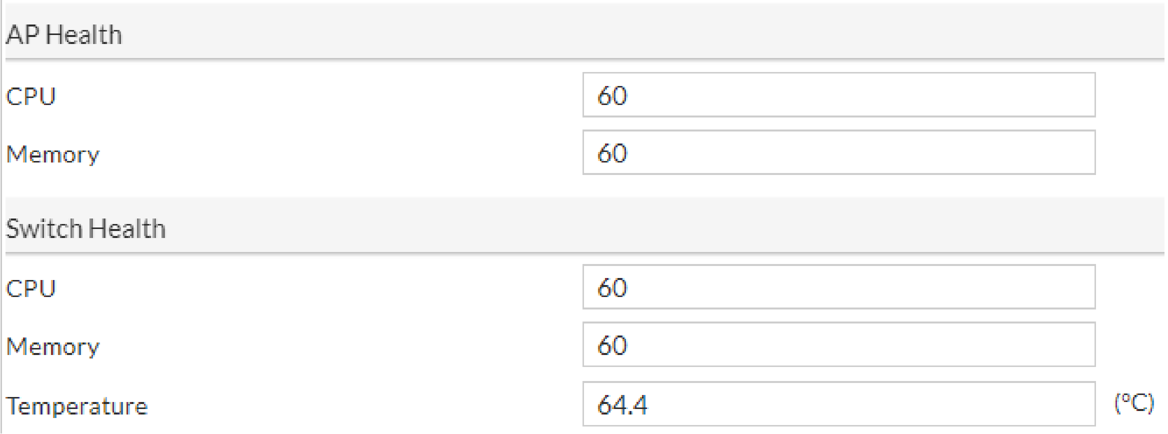
Association Time	300	ms
Authentication Time	300	ms
DHCP Time	300	ms
DNS Time	300	ms

AP Health and Switch Health

These configurations determine the health of the AP and switch based on the following set thresholds and display relevant statistics in the Monitor on page 15 tab.

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

- **Temperature**



AP Health

CPU	60	
Memory	60	

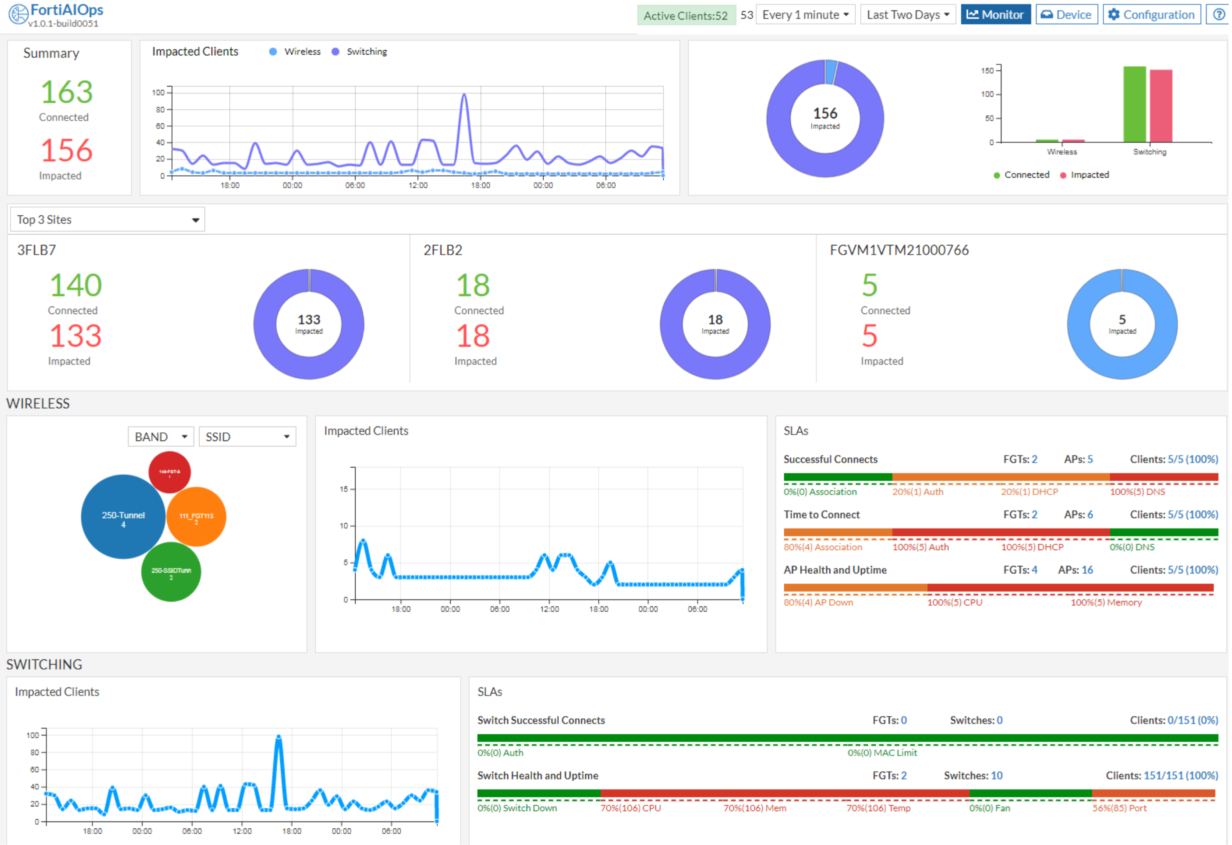
Switch Health

CPU	60	
Memory	60	
Temperature	64.4	(°C)

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

Monitor

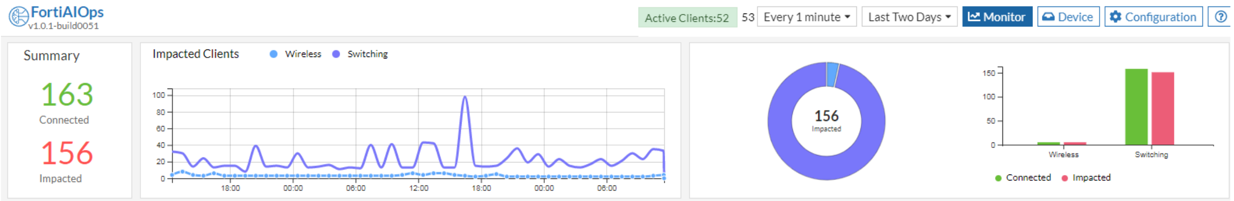
The FortiAIOps provides a comprehensive dashboard with detailed statistics and visualization for the wireless and switching clients. The information presented in the dashboard for impacted clients (failure to associate, authenticate, get a DHCP address, resolve DNS, and pass traffic on the wireless network) is pivotal for monitoring device health for diagnostic purpose. The dashboards present data in four panels - **Summary**, **Top 3 Sites**, **Wireless**, and **Switching**. Data is displayed in a series of charts and graphs, that you can filter based on time duration. Dashboard data is refreshed at a configurable interval.



- Summary on page 15
- Top 3 Sites on page 16
- Wireless on page 16
- Switching on page 20

Summary

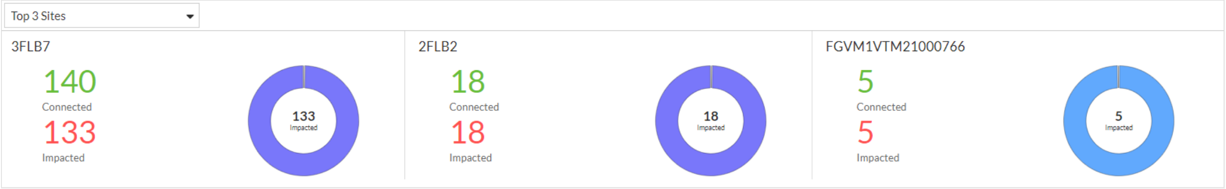
The **Summary** panels displays data in charts and statistics for the total number of connected and impacted clients for switching and wireless. The total number of **Active Clients** is also displayed.



Top 3 Sites

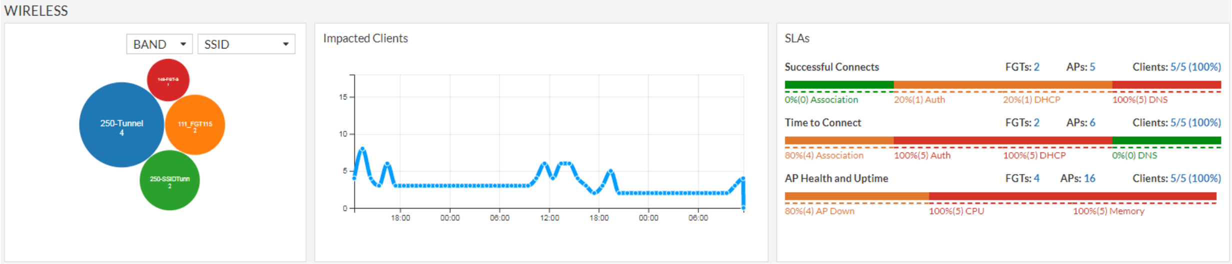
The **Top 3 Sites** panel allows you to view client data related to the top 3 FortiGate controllers with the highest number of associated clients. It also displays the total number of connected and impacted clients for each FortiGate controller.

You can view collective data for all 3 sites or select any one to view data.



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.



Successful Connects FGTs: 2 APs: 5 Clients: 5/5 (100%)
0%(0) Association 20%(1) Auth 20%(1) DHCP 100%(5) DNS

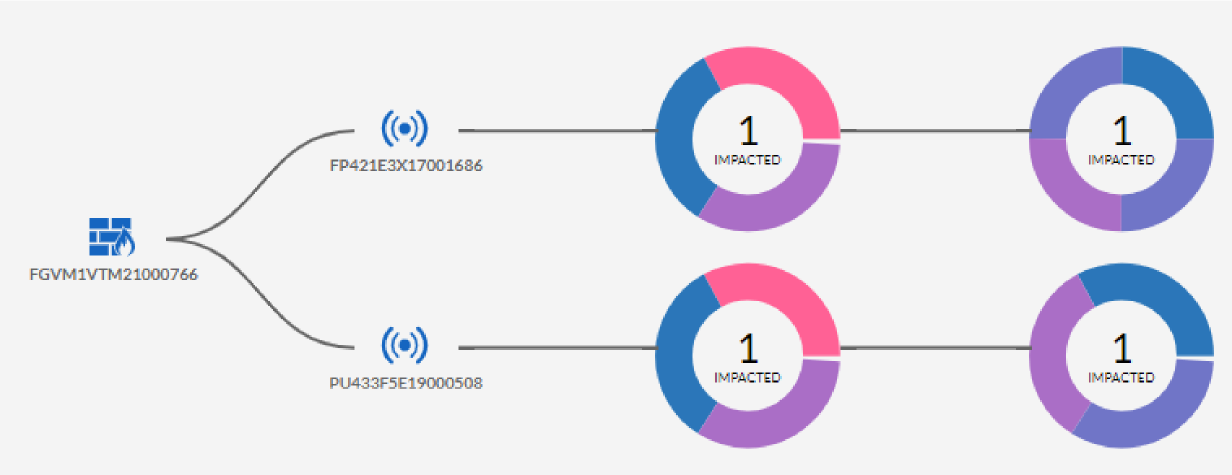
Time to Connect FGTs: 2 APs: 6 Clients: 5/5 (100%)
80%(4) Association 100%(5) Auth 100%(5) DHCP 0%(0) DNS

AP Health and Uptime FGTs: 4 APs: 16 Clients: 5/5 (100%)
80%(4) AP Down 100%(5) CPU 100%(5) Memory

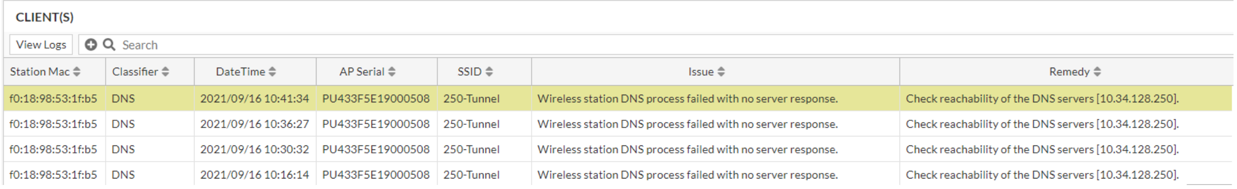
- **Successful Connects** - Displays the failed/unsuccessful client connections based on different stages of connection to a network. For example, association failures due to low RSSI, authentication failures due to unreachable RADIUS server, DHCP failure due to a DHCP server process crash, or DNS failure due to an invalid DNS domain.
- **Time to Connect** - Displays the clients that breach the configured SLA threshold values for these stages of connection, **Association**, **Authentication**, **DHCP**, and **DNS**. The actual value of time taken and configure **Time to Connect** threshold values are compared. See SLA Configurations on page 13.
- **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. See SLA Configurations on page 13.
- Topology on page 17
- Logs on page 18

Topology

In the **Successful Connects**, **Time to Connect**, and **Ap Health and Uptime** panels, the associated impacted FortiGate controller, AP, and client counts are displayed, click on any of these counts to view the topology. This is a sample topology view.

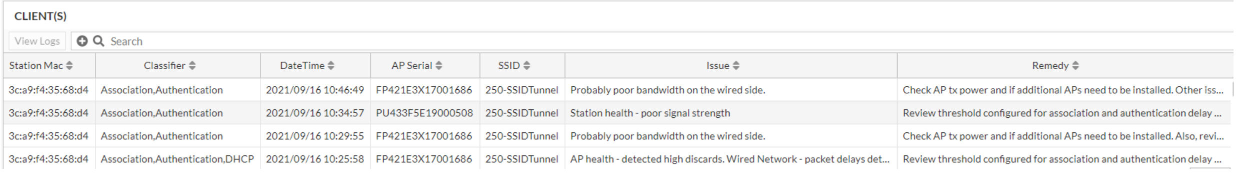


Furthermore, the impacted **Client** details such as the MAC address, the associated AP serial number and the SSID, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure are displayed. In this image impacted client details for **Successful Connects** are displayed.


CLIENT(S)

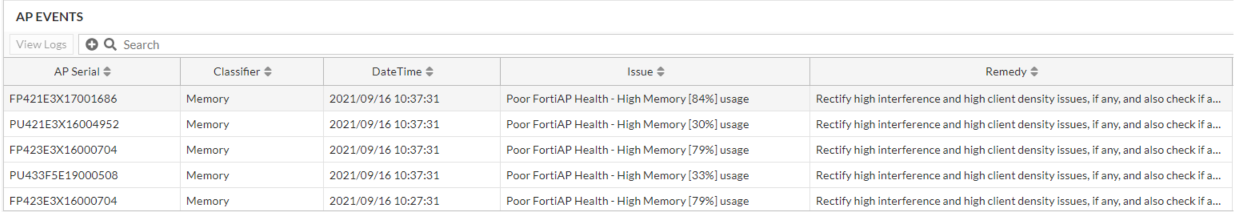
Station Mac	Classifier	DateTime	AP Serial	SSID	Issue	Remedy
f0:18:98:53:1f:b5	DNS	2021/09/16 10:41:34	PU433F5E19000508	250-Tunnel	Wireless station DNS process failed with no server response.	Check reachability of the DNS servers [10.34.128.250].
f0:18:98:53:1f:b5	DNS	2021/09/16 10:36:27	PU433F5E19000508	250-Tunnel	Wireless station DNS process failed with no server response.	Check reachability of the DNS servers [10.34.128.250].
f0:18:98:53:1f:b5	DNS	2021/09/16 10:30:32	PU433F5E19000508	250-Tunnel	Wireless station DNS process failed with no server response.	Check reachability of the DNS servers [10.34.128.250].
f0:18:98:53:1f:b5	DNS	2021/09/16 10:16:14	PU433F5E19000508	250-Tunnel	Wireless station DNS process failed with no server response.	Check reachability of the DNS servers [10.34.128.250].

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


CLIENT(S)

Station Mac	Classifier	DateTime	AP Serial	SSID	Issue	Remedy
3c:a9:f4:35:68:d4	Association,Authentication	2021/09/16 10:46:49	FP421E3X17001686	250-SSIDTunnel	Probably poor bandwidth on the wired side.	Check AP tx power and if additional APs need to be installed. Other iss...
3c:a9:f4:35:68:d4	Association,Authentication	2021/09/16 10:34:57	PU433F5E19000508	250-SSIDTunnel	Station health - poor signal strength	Review threshold configured for association and authentication delay ...
3c:a9:f4:35:68:d4	Association,Authentication	2021/09/16 10:29:55	FP421E3X17001686	250-SSIDTunnel	Probably poor bandwidth on the wired side.	Check AP tx power and if additional APs need to be installed. Also, revi...
3c:a9:f4:35:68:d4	Association,Authentication,DHCP	2021/09/16 10:25:58	FP421E3X17001686	250-SSIDTunnel	AP health - detected high discards. Wired Network - packet delays det...	Review threshold configured for association and authentication delay ...

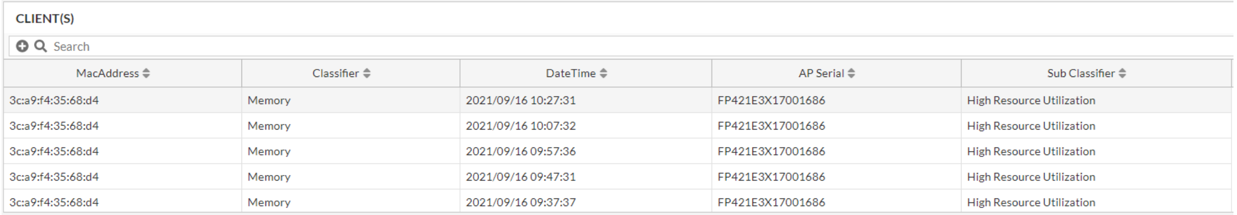
In the **Ap Health and Uptime**, the **AP Events** summary is displayed by default and provides details such as AP serial number, issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure are displayed.


AP EVENTS

AP Serial	Classifier	DateTime	Issue	Remedy
FP421E3X17001686	Memory	2021/09/16 10:37:31	Poor FortiAP Health - High Memory [84%] usage	Rectify high interference and high client density issues, if any, and also check if a...
PU421E3X16004952	Memory	2021/09/16 10:37:31	Poor FortiAP Health - High Memory [30%] usage	Rectify high interference and high client density issues, if any, and also check if a...
FP423E3X16000704	Memory	2021/09/16 10:37:31	Poor FortiAP Health - High Memory [79%] usage	Rectify high interference and high client density issues, if any, and also check if a...
PU433F5E19000508	Memory	2021/09/16 10:37:31	Poor FortiAP Health - High Memory [33%] usage	Rectify high interference and high client density issues, if any, and also check if a...
FP423E3X16000704	Memory	2021/09/16 10:27:31	Poor FortiAP Health - High Memory [79%] usage	Rectify high interference and high client density issues, if any, and also check if a...

In the displayed topology for wireless AP health, click on the client donut to view the impacted client details similar to the **Successful Connects** and **Time to Connect** panels.

In this image impacted client details for **AP Health and Uptime** are displayed.



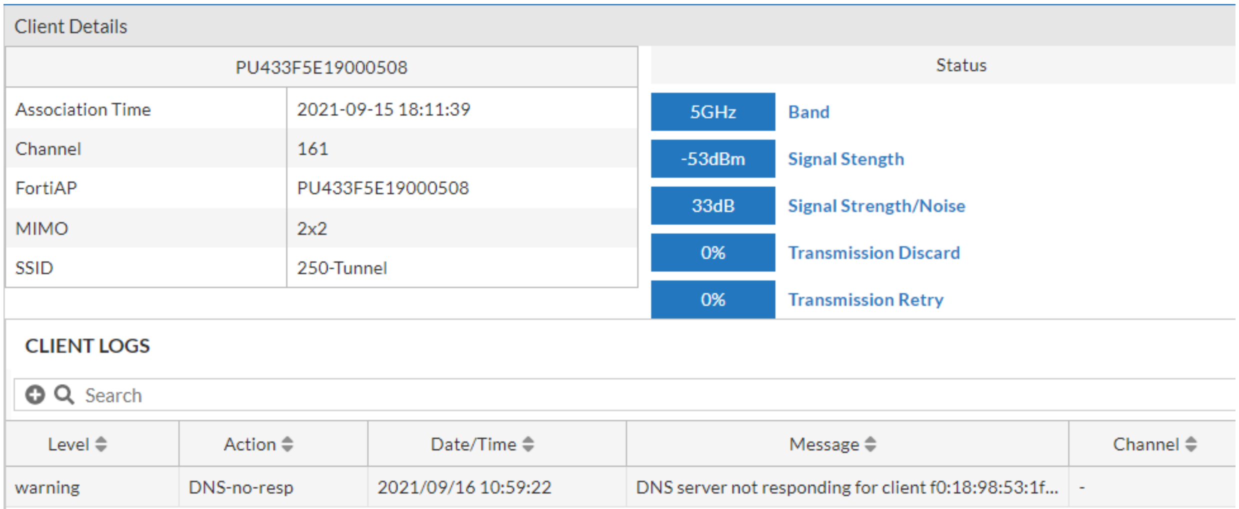
CLIENT(S)

MacAddress	Classifier	DateTime	AP Serial	Sub Classifier
3c:a9:f4:35:68:d4	Memory	2021/09/16 10:27:31	FP421E3X17001686	High Resource Utilization
3c:a9:f4:35:68:d4	Memory	2021/09/16 10:07:32	FP421E3X17001686	High Resource Utilization
3c:a9:f4:35:68:d4	Memory	2021/09/16 09:57:36	FP421E3X17001686	High Resource Utilization
3c:a9:f4:35:68:d4	Memory	2021/09/16 09:47:31	FP421E3X17001686	High Resource Utilization
3c:a9:f4:35:68:d4	Memory	2021/09/16 09:37:37	FP421E3X17001686	High Resource Utilization

Logs

In the impacted client details displayed for **Successful Connects** and **Time to Connect** panels, 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.

In this image logs for **Successful Connects** are displayed.



Client Details

PU433F5E19000508	
Association Time	2021-09-15 18:11:39
Channel	161
FortiAP	PU433F5E19000508
MIMO	2x2
SSID	250-Tunnel

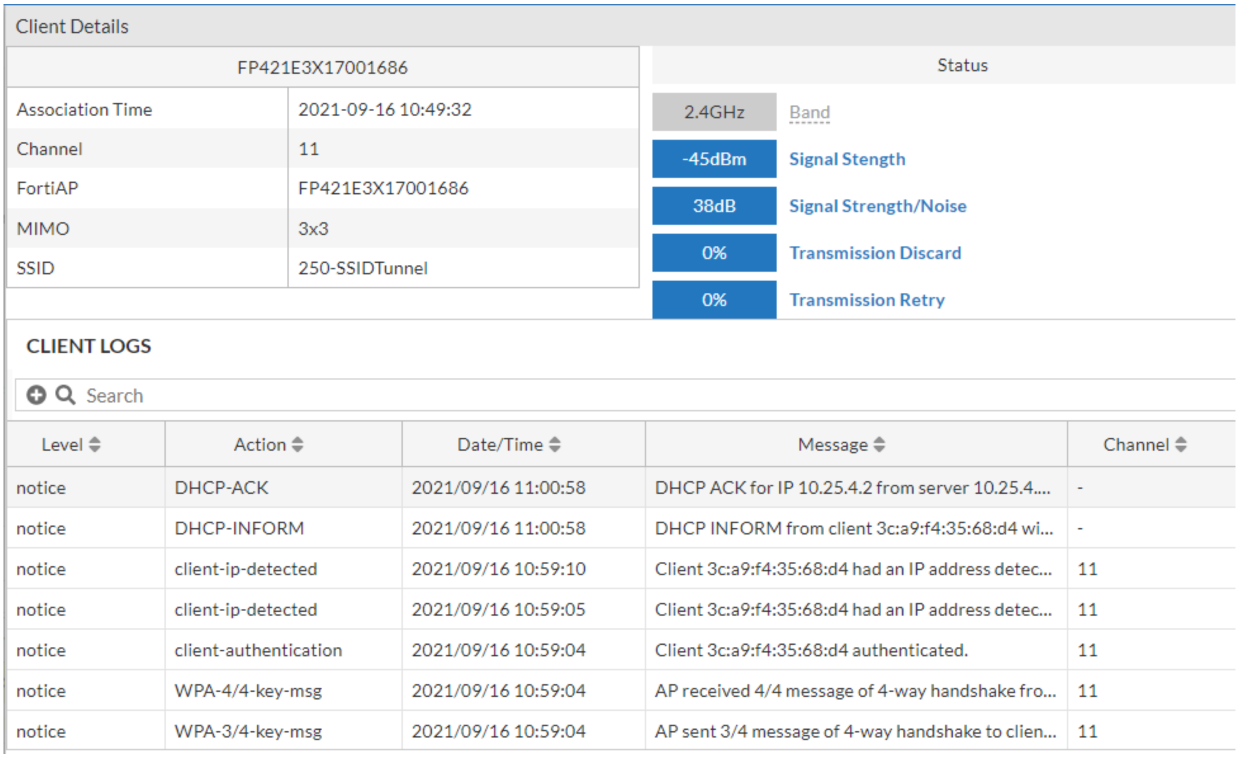
Status

5GHz	Band
-53dBm	Signal Stength
33dB	Signal Strength/Noise
0%	Transmission Discard
0%	Transmission Retry

CLIENT LOGS

Level	Action	Date/Time	Message	Channel
warning	DNS-no-resp	2021/09/16 10:59:22	DNS server not responding for client f0:18:98:53:1f...	-

In this image logs for **Time to Connect** are displayed.



Client Details

FP421E3X17001686	
Association Time	2021-09-16 10:49:32
Channel	11
FortiAP	FP421E3X17001686
MIMO	3x3
SSID	250-SSIDTunnel

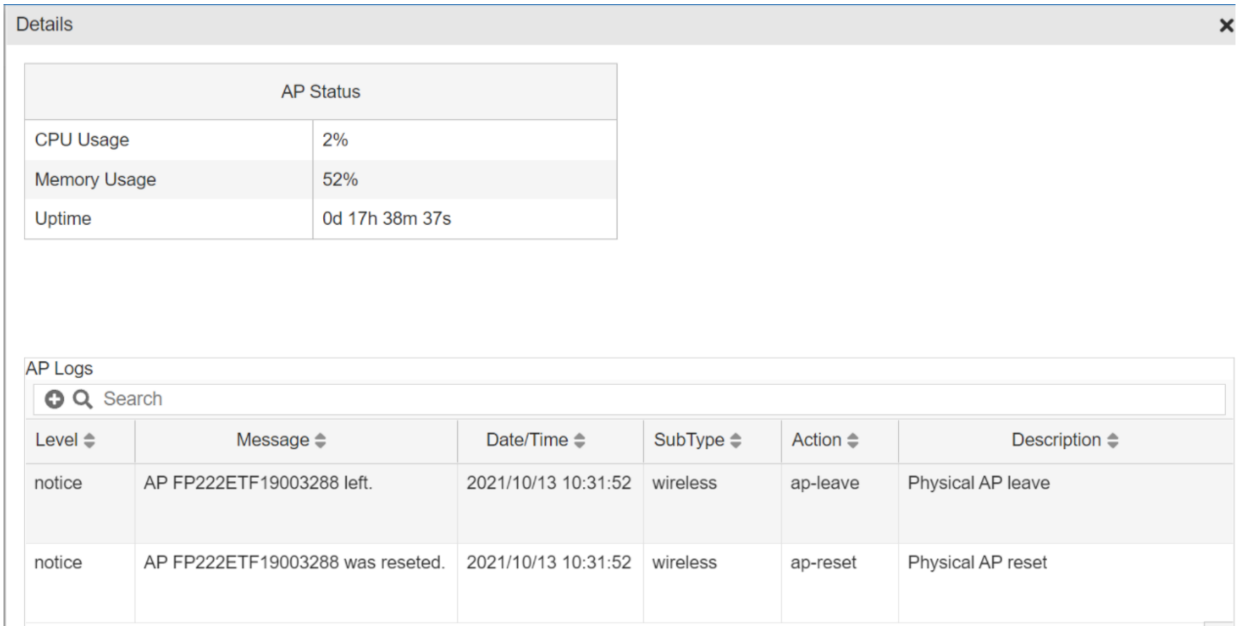
Status	
2.4GHz	Band
-45dBm	Signal Stength
38dB	Signal Strength/Noise
0%	Transmission Discard
0%	Transmission Retry

CLIENT LOGS

Level	Action	Date/Time	Message	Channel
notice	DHCP-ACK	2021/09/16 11:00:58	DHCP ACK for IP 10.25.4.2 from server 10.25.4....	-
notice	DHCP-INFORM	2021/09/16 11:00:58	DHCP INFORM from client 3c:a9:f4:35:68:d4 wi...	-
notice	client-ip-detected	2021/09/16 10:59:10	Client 3c:a9:f4:35:68:d4 had an IP address detec...	11
notice	client-ip-detected	2021/09/16 10:59:05	Client 3c:a9:f4:35:68:d4 had an IP address detec...	11
notice	client-authentication	2021/09/16 10:59:04	Client 3c:a9:f4:35:68:d4 authenticated.	11
notice	WPA-4/4-key-msg	2021/09/16 10:59:04	AP received 4/4 message of 4-way handshake fro...	11
notice	WPA-3/4-key-msg	2021/09/16 10:59:04	AP sent 3/4 message of 4-way handshake to clien...	11

In the AP events displayed for the **Ap Health and Uptime** panel, select an event and click **View Logs**. The logs display details based on specific events triggered by FortiAP, FortiSwitch, and/or FortiGate.

For AP health related events like poor CPU and memory, the AP status and logs are displayed.



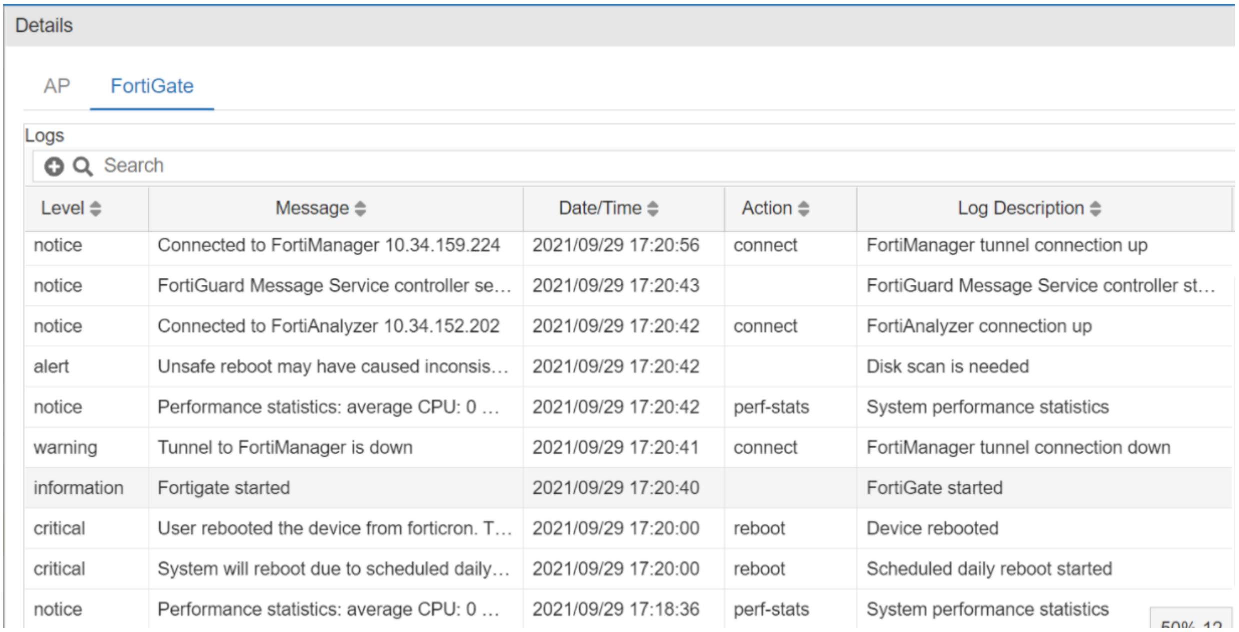
Details

AP Status	
CPU Usage	2%
Memory Usage	52%
Uptime	0d 17h 38m 37s

AP Logs

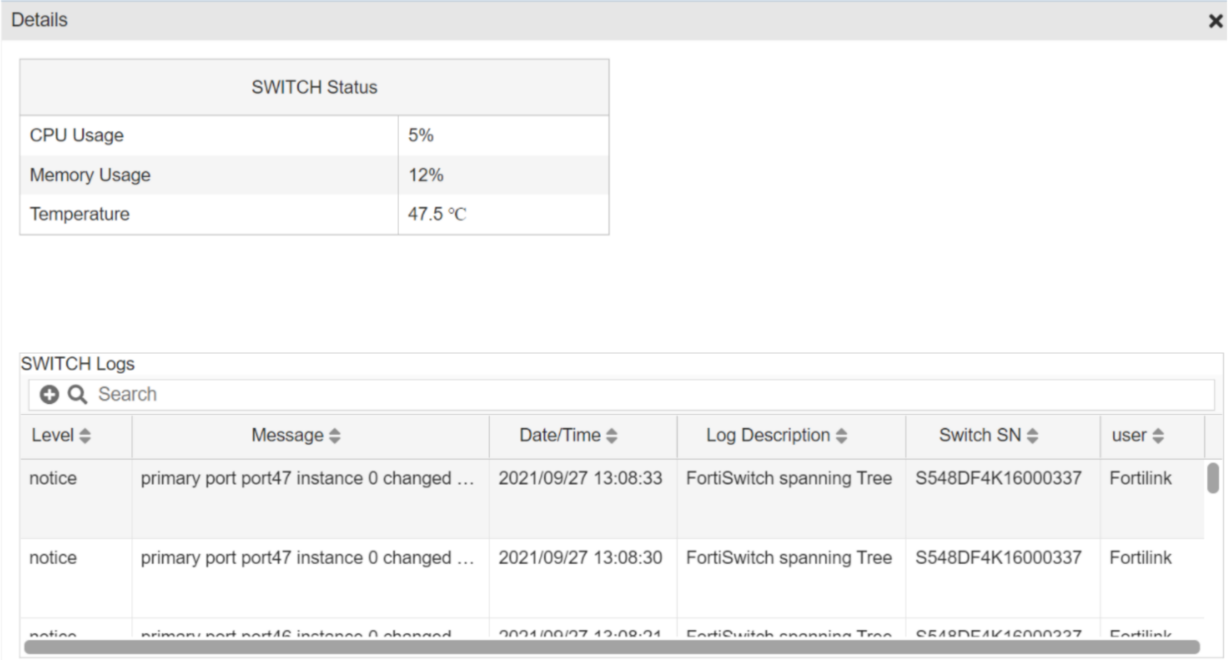
Level	Message	Date/Time	SubType	Action	Description
notice	AP FP222ETF19003288 left.	2021/10/13 10:31:52	wireless	ap-leave	Physical AP leave
notice	AP FP222ETF19003288 was reseted.	2021/10/13 10:31:52	wireless	ap-reset	Physical AP reset

For AP down events triggered due to FortiAP/FortiGate failure, the AP status and logs, and FortiGate logs are displayed.



Level	Message	Date/Time	Action	Log Description
notice	Connected to FortiManager 10.34.159.224	2021/09/29 17:20:56	connect	FortiManager tunnel connection up
notice	FortiGuard Message Service controller se…	2021/09/29 17:20:43		FortiGuard Message Service controller st…
notice	Connected to FortiAnalyzer 10.34.152.202	2021/09/29 17:20:42	connect	FortiAnalyzer connection up
alert	Unsafe reboot may have caused inconsis…	2021/09/29 17:20:42		Disk scan is needed
notice	Performance statistics: average CPU: 0 …	2021/09/29 17:20:42	perf-stats	System performance statistics
warning	Tunnel to FortiManager is down	2021/09/29 17:20:41	connect	FortiManager tunnel connection down
information	Fortigate started	2021/09/29 17:20:40		FortiGate started
critical	User rebooted the device from forticron. T…	2021/09/29 17:20:00	reboot	Device rebooted
critical	System will reboot due to scheduled daily…	2021/09/29 17:20:00	reboot	Scheduled daily reboot started
notice	Performance statistics: average CPU: 0 …	2021/09/29 17:18:36	perf-stats	System performance statistics

For AP down events triggered due to FortiSwitch related failure, the FortiSwitch status and logs are displayed.

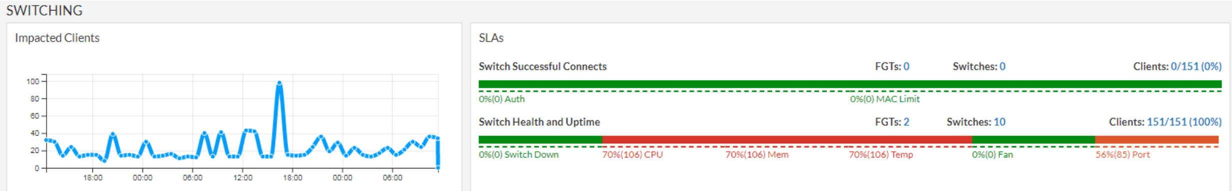


SWITCH Status	
CPU Usage	5%
Memory Usage	12%
Temperature	47.5 ℃

Level	Message	Date/Time	Log Description	Switch SN	user
notice	primary port port47 instance 0 changed …	2021/09/27 13:08:33	FortiSwitch spanning Tree	S548DF4K16000337	Fortilink
notice	primary port port47 instance 0 changed …	2021/09/27 13:08:30	FortiSwitch spanning Tree	S548DF4K16000337	Fortilink
notice	primary port port46 instance 0 changed	2021/09/27 13:08:21	FortiSwitch spanning Tree	S548DF4K16000337	Fortilink

Switching

The Switching panel displays the total number of impacted clients and SLA data.



SWITCHING

SLAs

Switch Successful Connects FGTs: 0 Switches: 0 Clients: 0/151 (0%)

0%(0) Auth 0%(0) MAC Limit

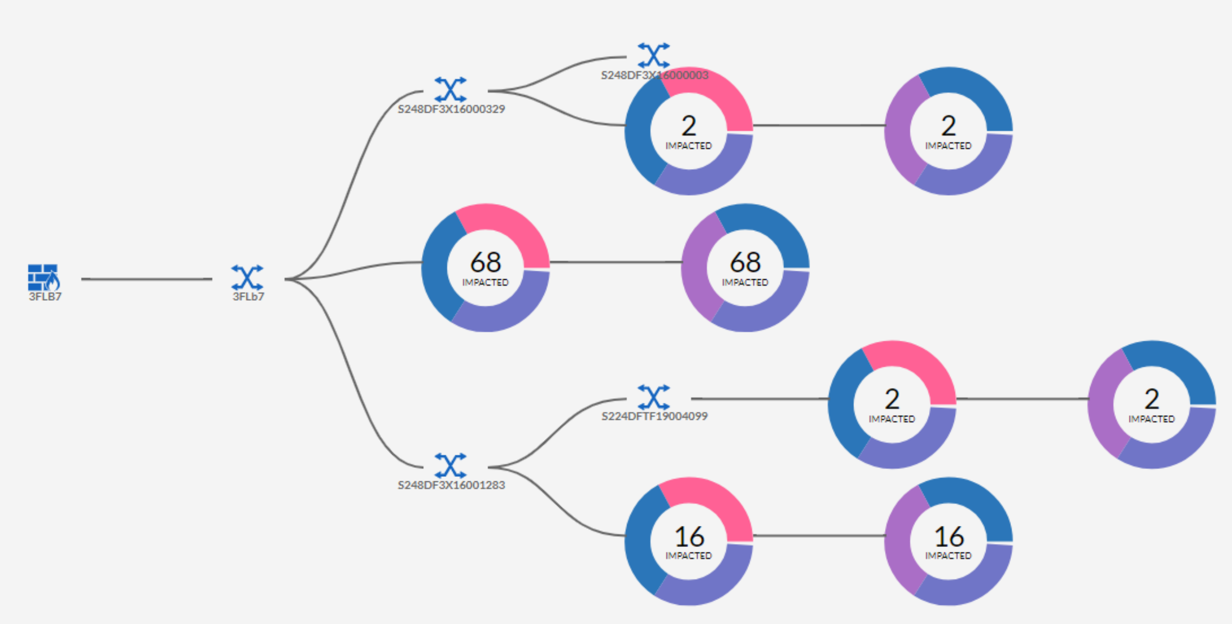
Switch Health and Uptime FGTs: 2 Switches: 10 Clients: 151/151 (100%)

0%(0) Switch Down 70%(106) CPU 70%(106) Mem 70%(106) Temp 0%(0) Fan 56%(85) Port

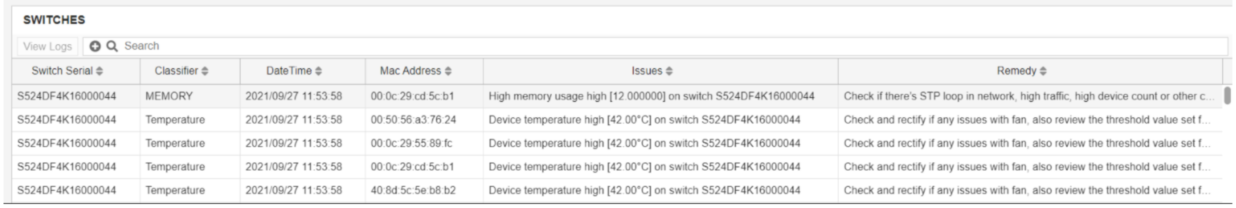
- **Switch Successful Connects** - Displays the failed/unsuccessful client connections based on authentication events such as MAC authentication and 801x authentication and MAC learning limit.
- **Switch Health and Uptime** - Displays the switch health based on the configured switch health threshold values and the status of the switch (Up/Down).
- Topology on page 21
- Logs on page 22

Topology

The associated impacted FortiGate controller, switch, and client count is also displayed, click on each of these counts to view the 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.



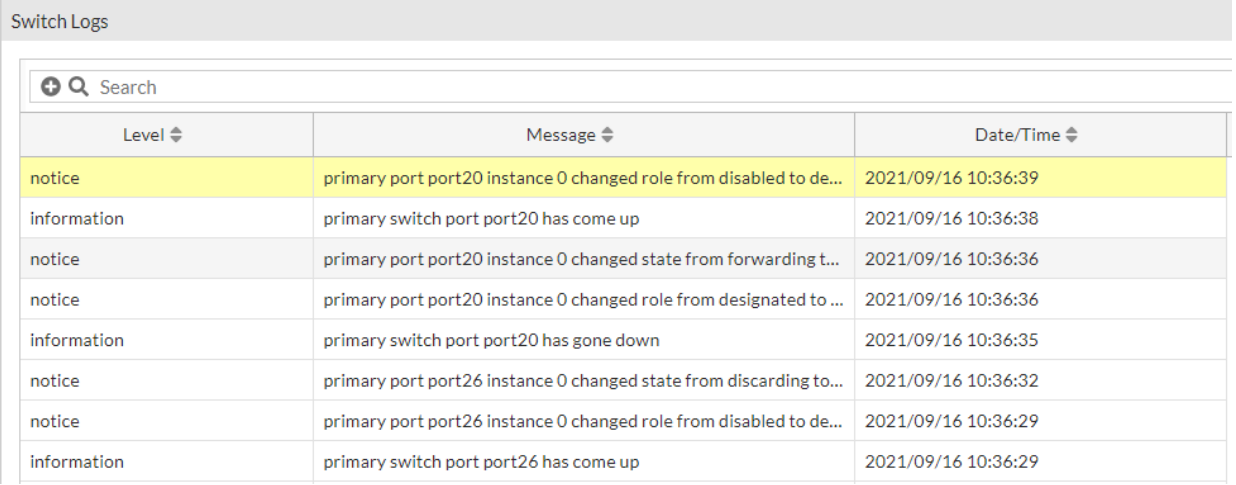
SWITCHES

View Logs ⊕ Search

Switch Serial	Classifier	DateTime	Mac Address	Issues	Remedy
S524DF4K16000044	MEMORY	2021/09/27 11:53:58	00:0c:29:cd:5c:b1	High memory usage high [12.000000] on switch S524DF4K16000044	Check if there's STP loop in network, high traffic, high device count or other c...
S524DF4K16000044	Temperature	2021/09/27 11:53:58	00:50:56:a3:76:24	Device temperature high [42.00°C] on switch S524DF4K16000044	Check and rectify if any issues with fan, also review the threshold value set f...
S524DF4K16000044	Temperature	2021/09/27 11:53:58	00:0c:29:55:89:fc	Device temperature high [42.00°C] on switch S524DF4K16000044	Check and rectify if any issues with fan, also review the threshold value set f...
S524DF4K16000044	Temperature	2021/09/27 11:53:58	00:0c:29:cd:5c:b1	Device temperature high [42.00°C] on switch S524DF4K16000044	Check and rectify if any issues with fan, also review the threshold value set f...
S524DF4K16000044	Temperature	2021/09/27 11:53:58	40:8d:5c:5e:b8:b2	Device temperature high [42.00°C] on switch S524DF4K16000044	Check and rectify if any issues with fan, also review the threshold value set f...

Logs

Select a particular switch and click **View Logs**, 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.

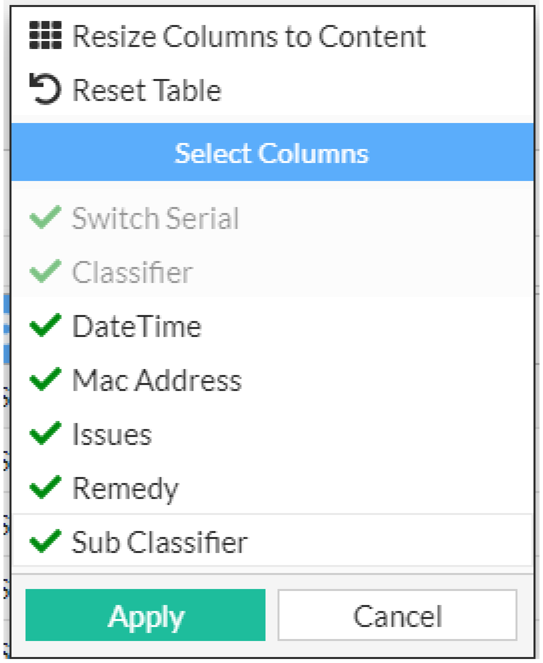


Switch Logs

Level	Message	Date/Time
notice	primary port port20 instance 0 changed role from disabled to de...	2021/09/16 10:36:39
information	primary switch port port20 has come up	2021/09/16 10:36:38
notice	primary port port20 instance 0 changed state from forwarding t...	2021/09/16 10:36:36
notice	primary port port20 instance 0 changed role from designated to ...	2021/09/16 10:36:36
information	primary switch port port20 has gone down	2021/09/16 10:36:35
notice	primary port port26 instance 0 changed state from discarding to...	2021/09/16 10:36:32
notice	primary port port26 instance 0 changed role from disabled to de...	2021/09/16 10:36:29
information	primary switch port port26 has come up	2021/09/16 10:36:29

Table Filter

The data displayed in tabular format in the monitor page is filterable based on columns, you can group data by a specific column or filter data for specific values.



- ✓ Switch Serial
- ✓ Classifier
- ✓ DateTime
- ✓ Mac Address
- ✓ Issues
- ✓ Remedy
- ✓ Sub Classifier

Special Notes

The following are applicable in this release of FortiAIOps.

- FortiAIOps data backup and restore is not supported.
- Client raw logs are displayed are not specific to the particular failure.
- Donuts in the Monitor page are not click-able.