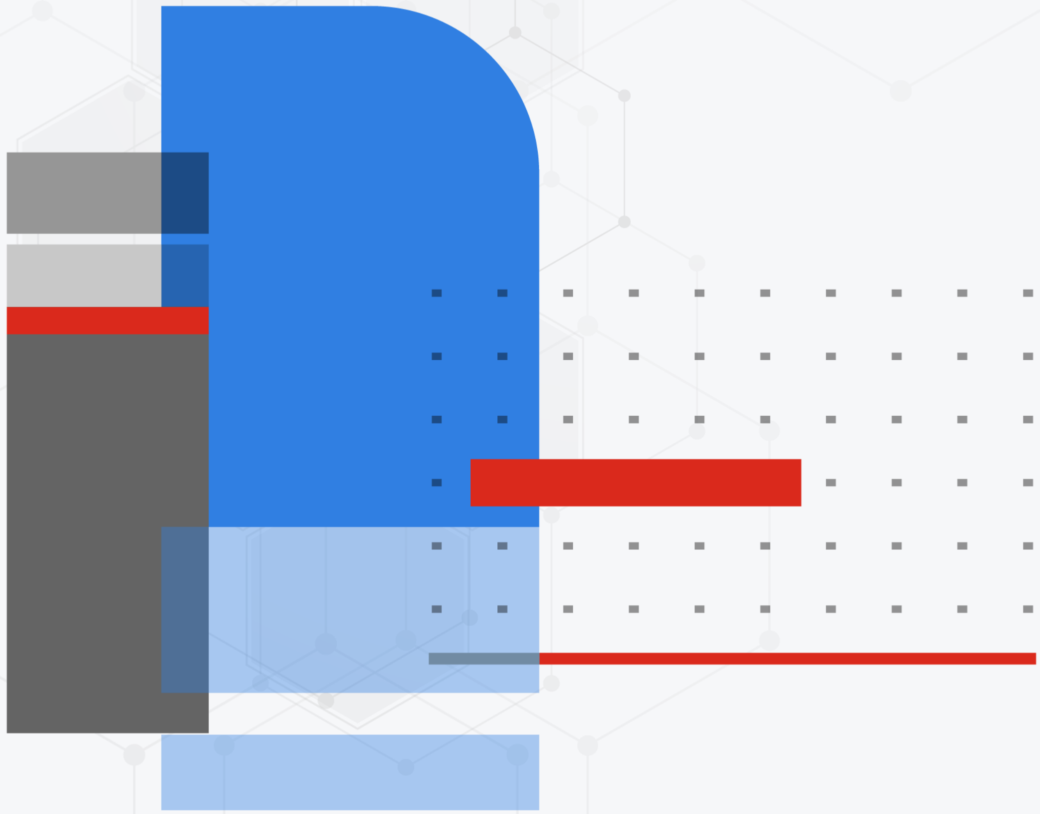
FORTINET

New Features

FortiAIOps 3.2.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

Feb 05, 2026
FortiAIOps 3.2.0 New Features
83-320-1224501-20260205

TABLE OF CONTENTS

Change log 4
About the Release 5
AI-Driven Automated Radio Resource Provisioning (AI-ARRP) 6
  Filtering 7
  Monitoring Widgets 8
    Impacted Radio Forecast 8
    Radio Health Summary 8
    Channel Change Events 9
    Channel Change Reason 10
  Detailed Analysis and Optimization 11
  Disabling AI-ARRP 15
  Logging and Diagnostics 16
Enhanced Wi-Fi Maps 18
FortiExtender Monitoring and Diagnostics 38
Advanced Alert Acknowledgement 43
AI Insights for Network Health Monitoring 46
Enhanced Monitoring for Wireless Clients 48
Fabric Connectors: Deployment Mode Selection 52
Packet Capture Analysis using FortiAI (Generative AI Assistant) 53
Remote Authentication 57
Dashboard Filter Persistence 58

Change log

Date	Change description
2025-12-15	FortiAIOps release 3.2.0 document.
2026-01-07	Updated AI-Driven Automated Radio Resource Provisioning (AI-ARRP) section.
2026-02-05	Updated Fabric Connectors: Deployment Mode Selection section.

About the Release

This release introduces the following new features:

- AI-Driven Automated Radio Resource Provisioning (AI-ARRP)
- Enhanced Wi-Fi Maps
- FortiExtender Monitoring and Diagnostics
- Advanced Alert Acknowledgement
- AI Insights for Network Health Monitoring
- Enhanced Monitoring for Wireless Clients
- Fabric Connectors: Deployment Mode Selection
- Packet Capture Analysis using FortiAI (Generative AI Assistant)
- Remote Authentication
- Dashboard Filter Persistence

AI-Driven Automated Radio Resource Provisioning (AI-ARRP)

This release introduces AI-ARRP, an advanced, AI-driven system that automates and optimizes the management and distribution of wireless channels across all Access Points (APs) monitored by FortiAIOps. The AI engine makes precise channel decisions by leveraging historical telemetry and deep insights gathered by FortiAIOps.

The accuracy of AI-ARRP stems from its ability to optimally score every available channel for each FortiAP radio. This scoring uses critical RF metrics, including noise levels, channel utilization, interfering APs, rogue APs, and spectral RSSI. FortiAIOps achieves this accuracy by analyzing real-time RF conditions along with up to two weeks of historical channel data to generate reliable channel scores and recommend a better channel for the AP radio.

To use the FortiAIOps AI-ARRP engine, you must enable both `ai-darrp-support` and `darrp` within the FortiAP (WTP) profile (see DARRP with FortiAIOps managed FortiGates).

Use the following commands:

```
config wireless-controller wtp-profile
   edit <name>
      config radio-1
         set ai-darrp-support enable
         set darrp enable
      next
   next
end
```

Note: By default, `ai-darrp-support` is disabled.

The combination of the `darrp` and `ai-darrp-support` commands determine how FortiGate and FortiAIOps handle channel selection and data collection.

`darrp`	`ai-darrp-support`	Description
disable	enable	Local DARRP is inactive. FortiAIOps collects telemetry data using GET REST-APIs but cannot make changes.
enable	enable	The FortiAIOps engine takes control. It collects data and actively triggers channel changes using POST REST-APIs.

Note:

- It is recommended to enable both `darrp` and `ai-darrp-support` to leverage the FortiAIOps AI-ARRP capabilities.
- You can enable AI-ARRP from FortiAIOps GUI for Non AI-ARRP radios. See Enable AI-ARRP.

Once enabled, the FortiAIOps AI-ARRP engine performs the following actions:

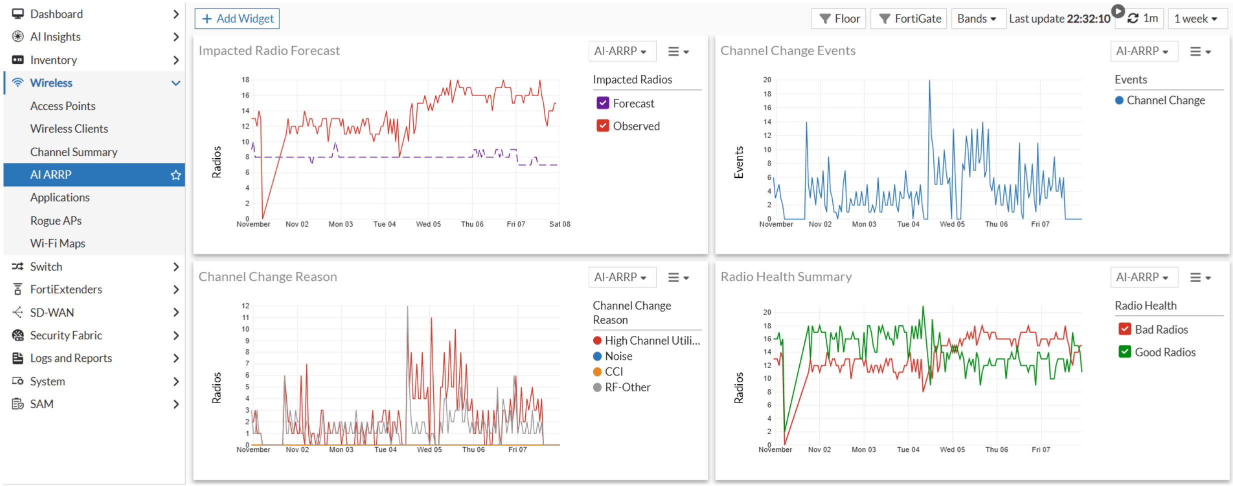
1. Data Collection: RF statistics for all channels on each AP radio are collected every minute.
2. Analysis and Daily Channel Health Forecast: The collected data is aggregated every hour, and the system evaluates the health of each available channel for that AP radio. The AI-ARRP model evaluates current

channel health metrics along with up to two weeks of historical RF data, and generates daily forecast of channel performance for each radio.

3. DARRP Schedule and Channel Validations: During the scheduled DARRP window on the FortiGate, AI-ARRP analyzes and performs a series of critical validation checks, including:
    - Channel availability based on the FortiAP profile
    - Mandatory regulatory compliance (country code and indoor/outdoor channel rules)
    - Non-overlapping channel requirements and channel bonding considerations
    - Channel failures related to Wireless SLAs and any radar detections
4. Final Channel Push: The finalized recommended channels for each radio are securely pushed to the FortiGate, and the FortiAPs use these updated channel assignments in their next channel planning cycle.

Note: AI-ARRP is only supported on FortiOS 7.6.5 and FortiAP version 7.6.3.

The new **AI ARRP** window is available under the **Wireless** menu.



Filtering

The **AI ARRP** window consists of four primary widgets and offers the following filtering capabilities:

Filters

Use the filters at the top to select **Floor**, **FortiGate**, and **Bands**.

- **Floor**: Select **Floor** filter and in the **Floor Selection** pane, choose the required **Site**, **Building** and **Floor** using the drop down.
- **FortiGate**: Select the **FortiGate** filter and from the **Dashboard Filters** pane select the required **FortiGate**.
- **Bands**: Select the necessary bands from the **Bands** filter.

Timeline

Select the monitoring timeline from the drop down. Choose between **4 hours**, **6 hours**, **1 day**, and **1 week**.

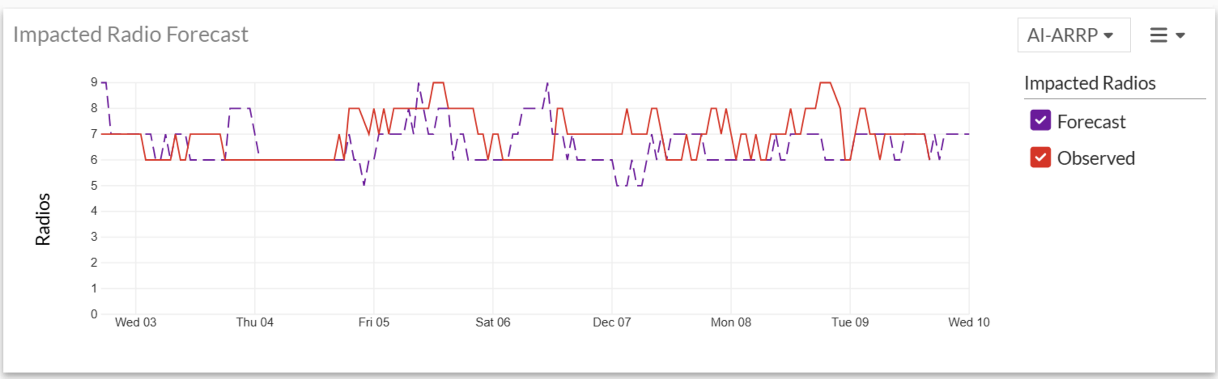
Monitoring Widgets

The **AI ARRP** window consists of four primary widgets designed to analyze the impact and reasons behind channel changes and radio health.

Note: To add the required widget to the dashboard, click **Add Widget** and from the **Wireless** > **AI ARRP** section, select a widget and click **+**.

Impacted Radio Forecast

This chart visualizes the difference between the observed (actual) and the forecast count of problematic radios by plotting the number of impacted radios against a specific time period.



The chart displays two key metrics:

- **Observed**: This line represents the real-time count of impacted radios that the system currently identifies as unhealthy or impacted.
- **Forecast**: This line shows the predicted count of impacted radios that the AI-ARRP model estimates will be impacted.

You can filter the displayed radio data using the drop-down menu to view specific management types:

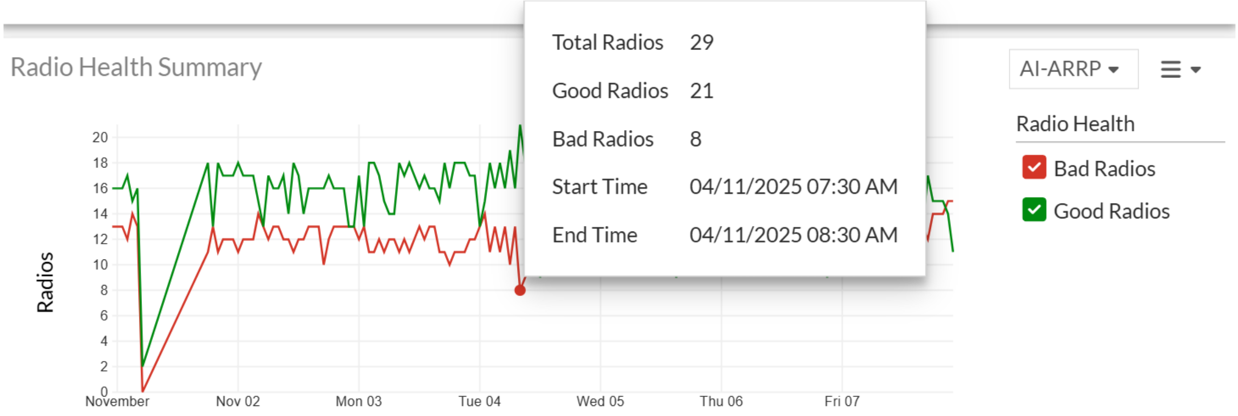
- **AI-ARRP**: Displays details only for radios where the AI-ARRP feature is enabled.
- **Non-AI-ARRP**: Includes radios where traditional DARRP is either enabled or disabled.
- **All**: Shows data covering both AI-ARRP managed radios and Non-AI-ARRP radios.

Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the details pane. See Detailed Analysis and Optimization.

Radio Health Summary

The **Radio Health Summary** chart shows the overall status of all AP radios by comparing how many radios are operating on good channels versus bad channels over time. Radios on good-performing channels are counted as **Good Radios**, while those running on poor-performing channels are counted as **Bad Radios**.



Total Radios 29
Good Radios 21
Bad Radios 8
Start Time 04/11/2025 07:30 AM
End Time 04/11/2025 08:30 AM

You can filter the displayed radio data using the drop-down menu to view specific management types:

- **AI-ARRP**: Displays details only for radios where the AI-ARRP feature is enabled.
- **Non-AI-ARRP**: Includes radios where traditional DARRP is either enabled or disabled.

Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the details pane. See Detailed Analysis and Optimization.

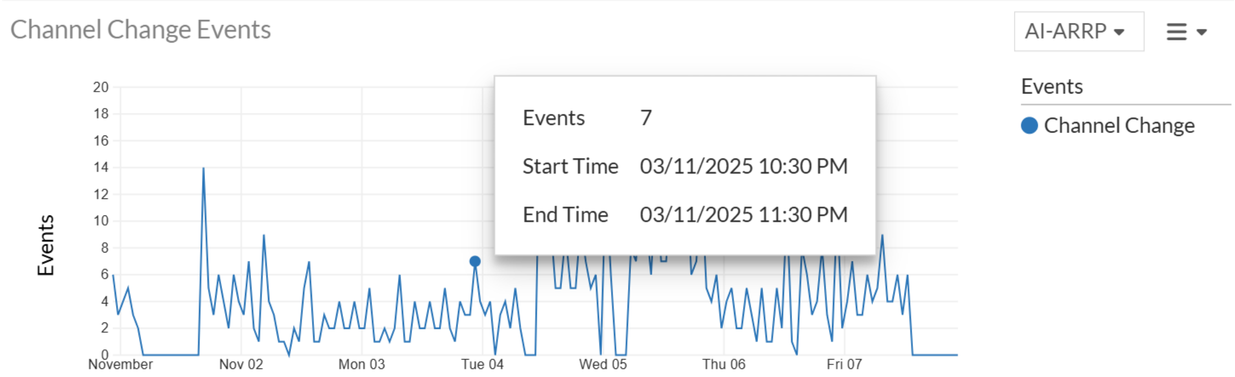
Channel Change Events

This chart provides detailed visibility into all channel change events triggered by the radio provisioning system. It captures channel changes initiated through both AI-ARRP from FortiAIOPs and DARRP from Fortigate.

When the **AI-ARRP** filter is applied, the chart shows all channel changes recommended by AI-ARRP.

When the **Non-AI-ARRP** filter is applied, it displays channel changes triggered by DARRP.

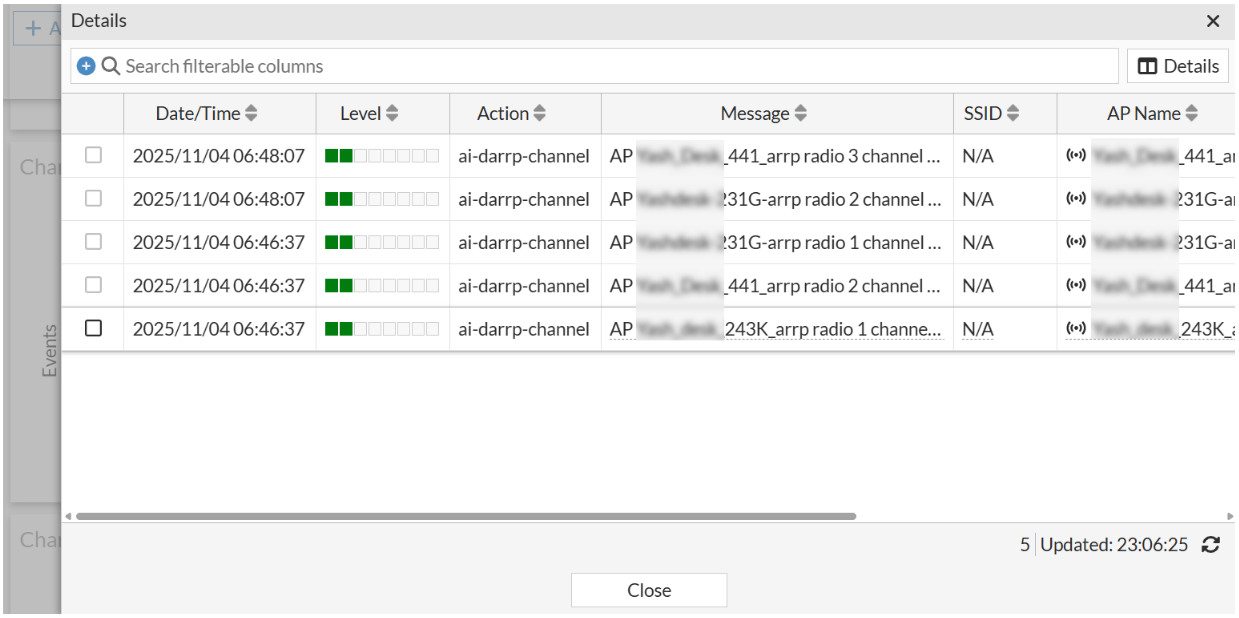
The chart shows how many times AP radios across the network switched their operating channel within the selected time period



Events 7
Start Time 03/11/2025 10:30 PM
End Time 03/11/2025 11:30 PM

Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the **Details** pane.

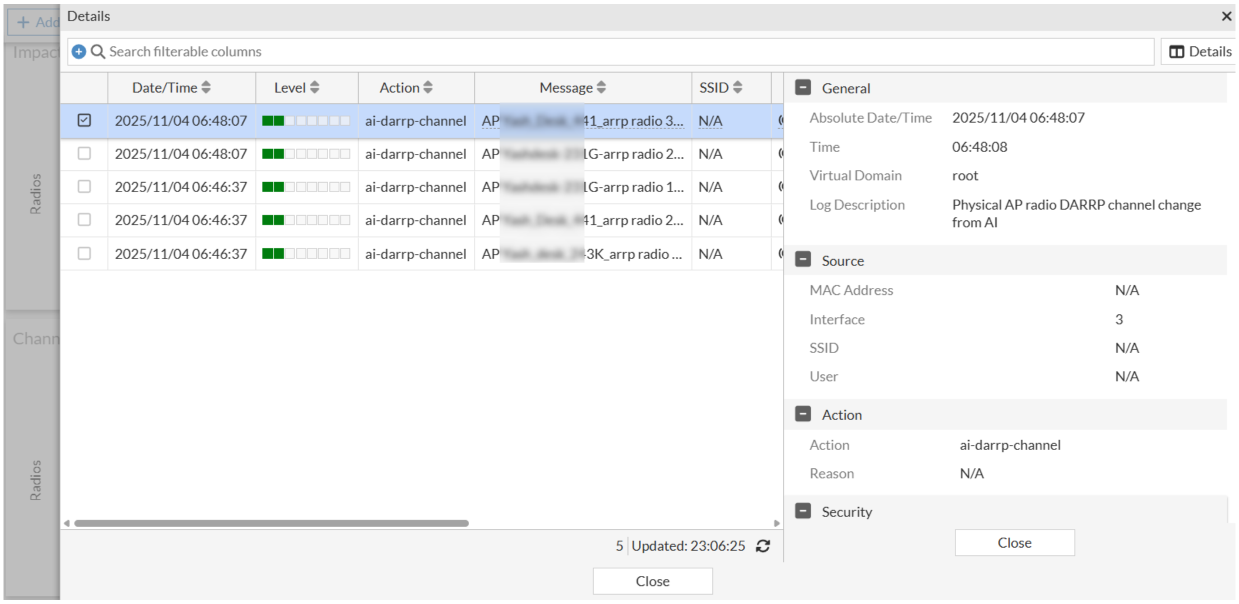


	Date/Time	Level	Action	Message	SSID	AP Name
☐	2025/11/04 06:48:07	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]_441_arrp radio 3 channel ...	N/A	[redacted]_441_ar
☐	2025/11/04 06:48:07	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]231G-arrp radio 2 channel ...	N/A	[redacted]231G-ar
☐	2025/11/04 06:46:37	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]231G-arrp radio 1 channel ...	N/A	[redacted]231G-ar
☐	2025/11/04 06:46:37	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]_441_arrp radio 2 channel ...	N/A	[redacted]_441_ar
☐	2025/11/04 06:46:37	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]_243K_arrp radio 1 channe...	N/A	[redacted]_243K_

5 Updated: 23:06:25

The table in the **Details** pane provide details such as **Date/Time**, **Level**, **Action**, **Message**, **SSID**, **AP Name**, **Log ID**, **FortiGate Serial Number**, and **Channel**.

Select an event and click Details icon to view further details.



	Date/Time	Level	Action	Message	SSID
☑	2025/11/04 06:48:07	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]41_arrp radio 3...	N/A
☐	2025/11/04 06:48:07	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]1G-arrp radio 2...	N/A
☐	2025/11/04 06:46:37	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]1G-arrp radio 1...	N/A
☐	2025/11/04 06:46:37	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]41_arrp radio 2...	N/A
☐	2025/11/04 06:46:37	🟩🟩⬜⬜⬜⬜⬜⬜	ai-darrp-channel	AP [redacted]3K_arrp radio ...	N/A

5 Updated: 23:06:25

General

Absolute Date/Time	2025/11/04 06:48:07
Time	06:48:08
Virtual Domain	root
Log Description	Physical AP radio DARRP channel change from AI

Source

MAC Address	N/A
Interface	3
SSID	N/A
User	N/A

Action

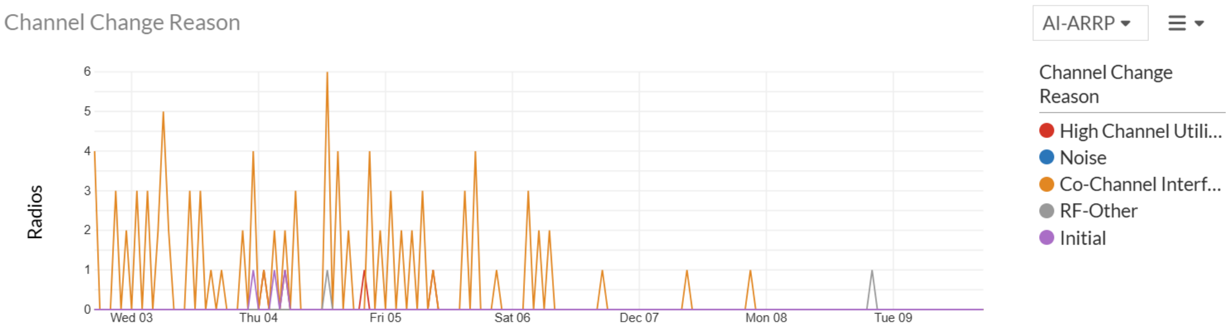
Action	ai-darrp-channel
Reason	N/A

Security

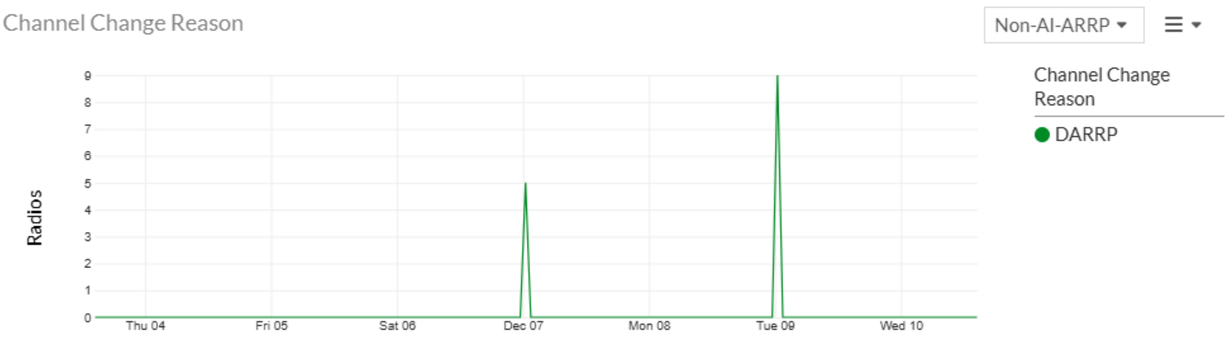
Channel Change Reason

This widget provides a detailed breakdown of the factors that prompted AI-ARRP to recommend a channel change, highlighting the key conditions that affected the health of the current operating channel. The reasons reported include:

- High Channel Utilization
- Noise
- Co-channel Interference (neighboring APs detected on overlapping channels)
- RF-Other (such as Spectral RSSI)
- Initial (channel change applied based on FortiGate results)



When the **Non-AI-ARRP** filter is applied, the widget displays the reason as DARRP, indicating that the channel change was recommended by FortiOS DARRP.

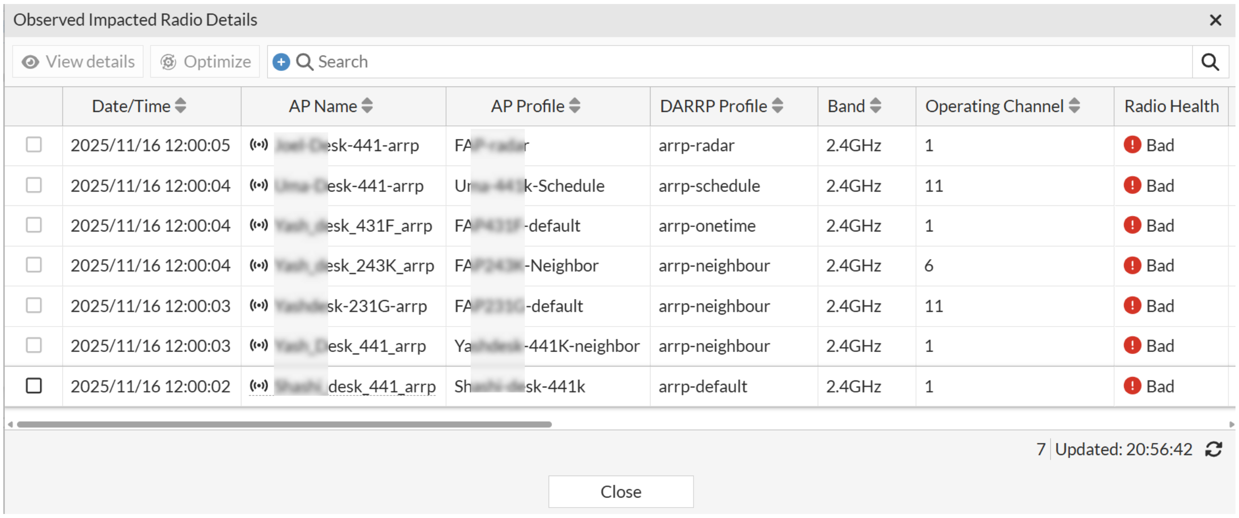


Hover over a data point on the chart to view more details.

Clicking on a data point on the chart opens the details pane. See Detailed Analysis and Optimization.

Detailed Analysis and Optimization

Clicking on a data point in the **Impacted Radio Forecast** or **Radio Health Summary** or **Channel Change Reason** charts opens a pane for detailed analysis and action.



Observed Impacted Radio Details

	Date/Time	AP Name	AP Profile	DARRP Profile	Band	Operating Channel	Radio Health
☐	2025/11/16 12:00:05	[redacted]esk-441-arrp	FA[redacted]r	arrp-radar	2.4GHz	1	Bad
☐	2025/11/16 12:00:04	[redacted]esk-441-arrp	U[redacted]k-Schedule	arrp-schedule	2.4GHz	11	Bad
☐	2025/11/16 12:00:04	[redacted]esk_431F_arrp	FA[redacted]-default	arrp-onetime	2.4GHz	1	Bad
☐	2025/11/16 12:00:04	[redacted]esk_243K_arrp	FA[redacted]-Neighbor	arrp-neighbour	2.4GHz	6	Bad
☐	2025/11/16 12:00:03	[redacted]sk-231G-arrp	FA[redacted]-default	arrp-neighbour	2.4GHz	11	Bad
☐	2025/11/16 12:00:03	[redacted]esk_441_arrp	Ya[redacted]-441K-neighbor	arrp-neighbour	2.4GHz	1	Bad
☐	2025/11/16 12:00:02	[redacted]desk_441_arrp	Sh[redacted]sk-441k	arrp-default	2.4GHz	1	Bad

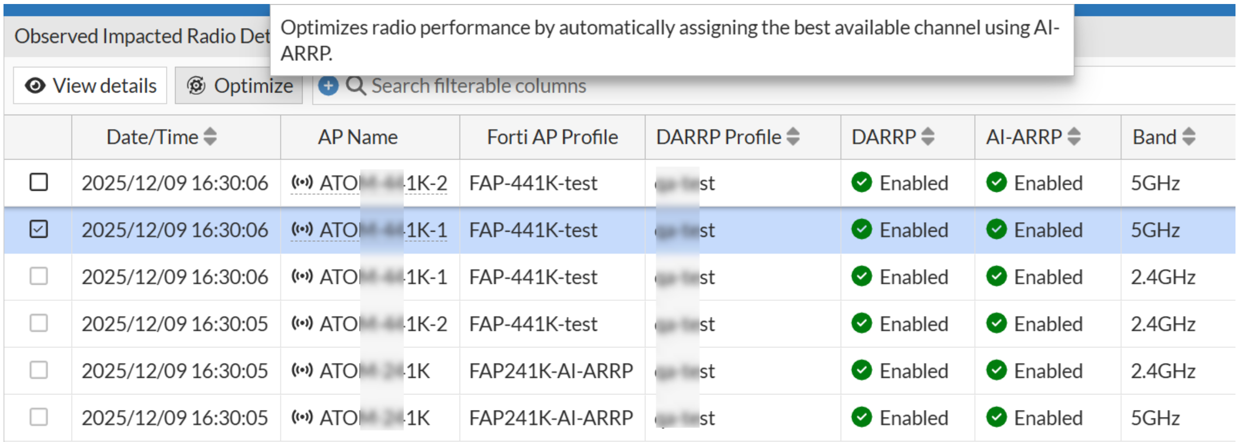
7 | Updated: 20:56:42

The table displays information such as **Date/Time**, **AP Name**, **AP Profile**, **DARRP Profile**, **Band**, **Operating Channel**, **Radio Health**, **Radio Health Summary**, **Radio ID**, **Channel Change Reason**, **FortiGate Name**, **AP Serial Number**, **FortiGate Serial Number**, and **Last Channel Change**.

Optimize

Select an AP radio and click **Optimize** to manually trigger an immediate channel planning on that radio. This action evaluates the current RF environment and recommends the most optimal operating channel. Unlike the scheduled AI-ARRP runs, this channel-planning operation occurs instantly and may impact connected clients if performed during business hours.

Note: Optimize can be performed only on radios impacted in last 1 hour.



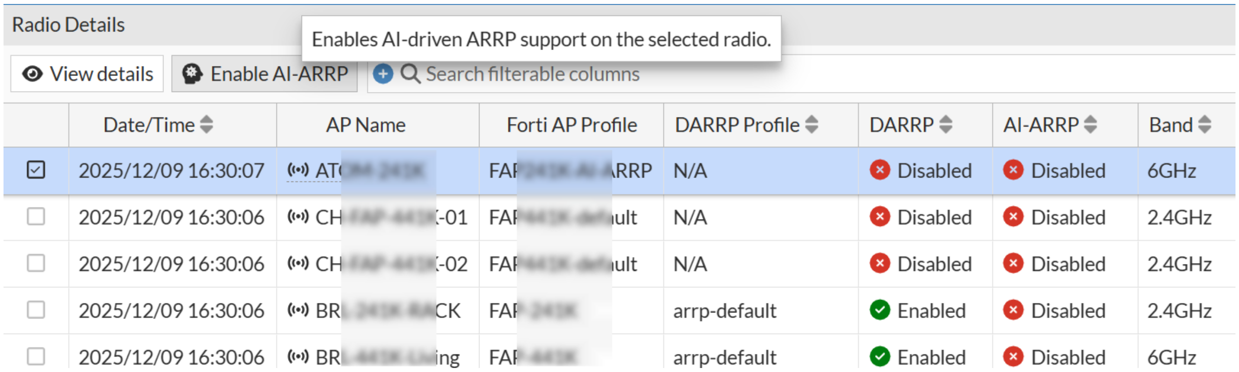
Observed Impacted Radio Det

Optimizes radio performance by automatically assigning the best available channel using AI-ARRP.

	Date/Time	AP Name	Forti AP Profile	DARRP Profile	DARRP	AI-ARRP	Band
☐	2025/12/09 16:30:06	ATO[redacted]1K-2	FAP-441K-test	[redacted]st	Enabled	Enabled	5GHz
☑	2025/12/09 16:30:06	ATO[redacted]1K-1	FAP-441K-test	[redacted]st	Enabled	Enabled	5GHz
☐	2025/12/09 16:30:06	ATO[redacted]1K-1	FAP-441K-test	[redacted]st	Enabled	Enabled	2.4GHz
☐	2025/12/09 16:30:05	ATO[redacted]1K-2	FAP-441K-test	[redacted]st	Enabled	Enabled	2.4GHz
☐	2025/12/09 16:30:05	ATO[redacted]1K	FAP241K-AI-ARRP	[redacted]st	Enabled	Enabled	2.4GHz
☐	2025/12/09 16:30:05	ATO[redacted]1K	FAP241K-AI-ARRP	[redacted]st	Enabled	Enabled	5GHz

Enable AI-ARRP

To enable AI-ARRP from FortiAIOps for Non AI-ARRP radios, select the Non AI-ARRP radios impacted in the last 1 hour and click **Enable AI-ARRP**.

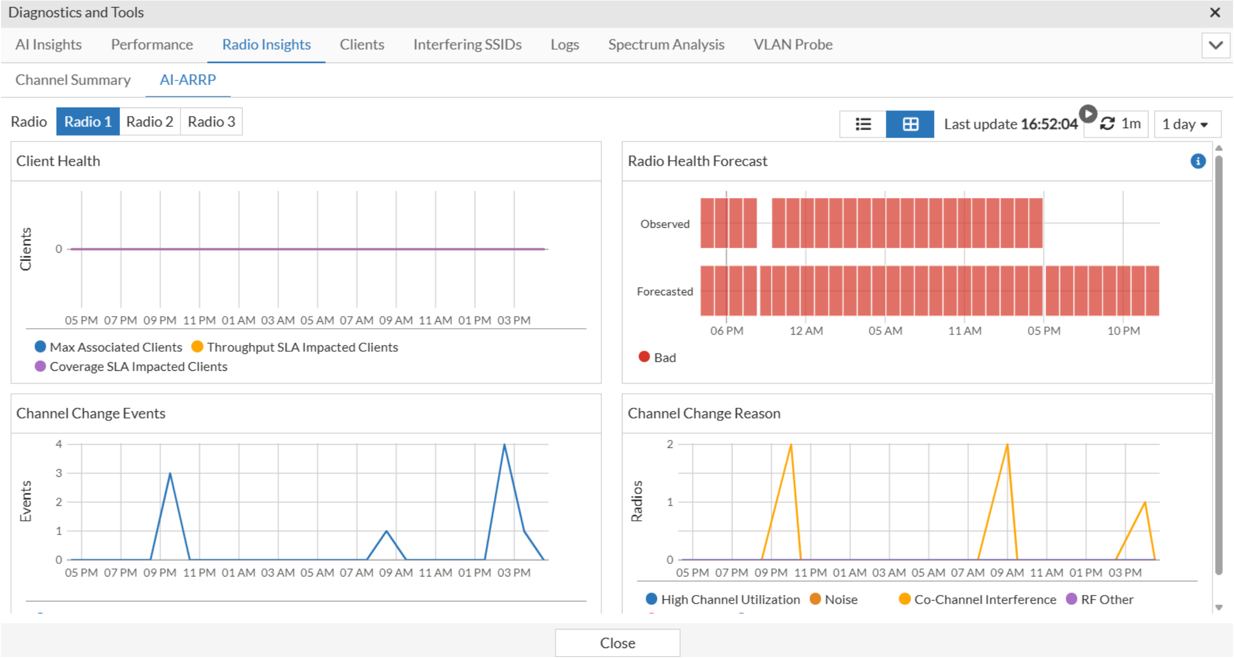

Radio Details
Enables AI-driven ARRP support on the selected radio.
View details
Enable AI-ARRP
Search filterable columns

	Date/Time	AP Name	Forti AP Profile	DARRP Profile	DARRP	AI-ARRP	Band
☑	2025/12/09 16:30:07	AT[redacted]	FAP[redacted]RRP	N/A	Disabled	Disabled	6GHz
☐	2025/12/09 16:30:06	CH[redacted]-01	FAP[redacted]ult	N/A	Disabled	Disabled	2.4GHz
☐	2025/12/09 16:30:06	CH[redacted]-02	FAP[redacted]ult	N/A	Disabled	Disabled	2.4GHz
☐	2025/12/09 16:30:06	BR[redacted]CK	FAP[redacted]	arrp-default	Enabled	Disabled	2.4GHz
☐	2025/12/09 16:30:06	BR[redacted]ing	FAP[redacted]	arrp-default	Enabled	Disabled	6GHz

View Details

Select and AP and click **View Details** to open the dedicated **Details** pane for the selected radio.

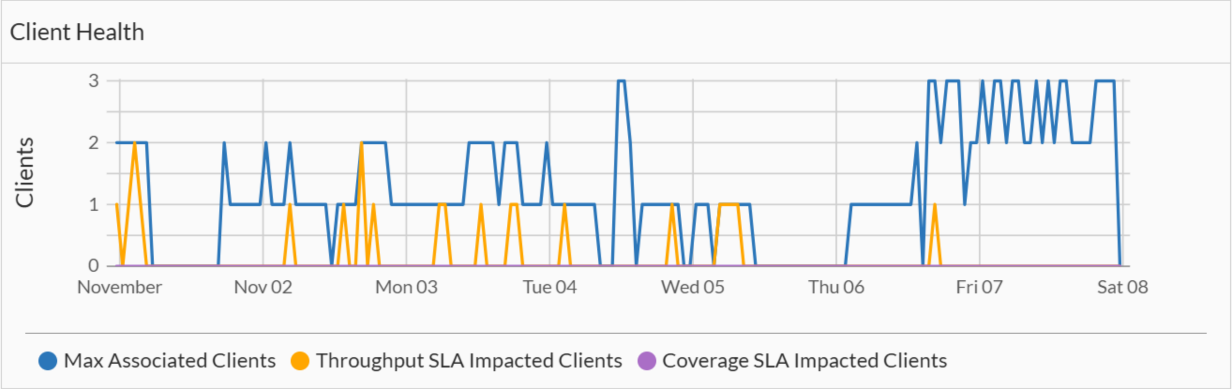
Note: Similar insights are available for individual Access Points on a per-radio basis by navigating to **Wireless** > **Access Points**. Select the desired AP, click **View Details**, and then go to the **Radio Insights** tab and the **AI-ARRP** sub-tab.



The following charts are displayed:

Client Health

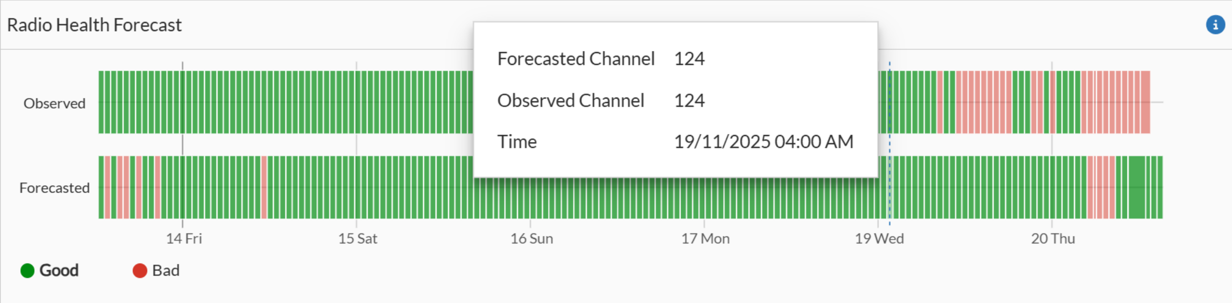
This chart tracks the following client-related issues over time.



- **Max Associated Clients**: Shows the maximum number of clients associated with this specific radio.
- **Throughput SLA Impacted Clients**: Tracks clients whose throughput is falling below the configured Service Level Agreement (SLA).
- **Coverage SLA Impacted Clients**: Tracks clients experiencing poor coverage.

Radio Health Forecast

This bar chart provides a visualization of the radio health over the monitored period.

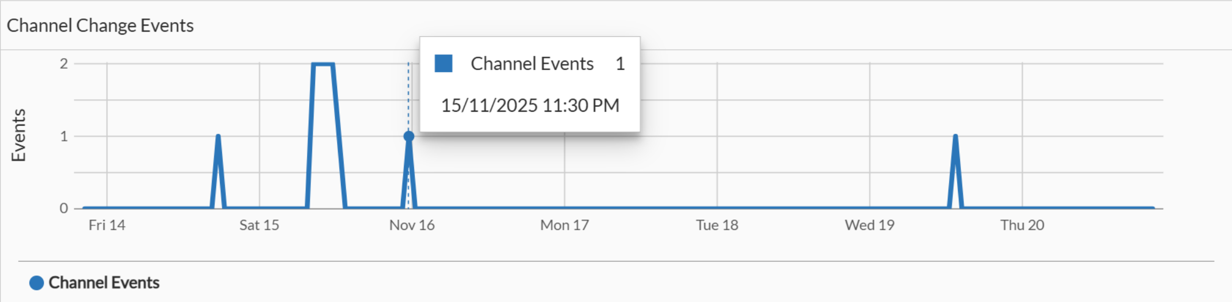


Forecasted Channel 124
Observed Channel 124
Time 19/11/2025 04:00 AM

- **Observed**: Shows the actual periods when the radio's health was good or bad on operating channel. Red bars indicate periods when the radio’s channel health was bad, while green bars represent periods when the radio was operating with good channel
- **Forecast**: Shows the periods when the AI-ARRP model predicted that the radio health on channel would be impacted. This helps evaluate the accuracy of the AI prediction against the observed reality.

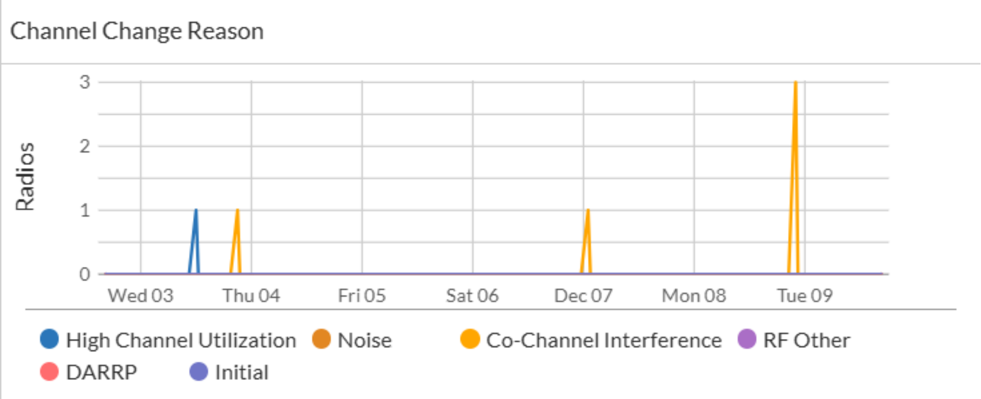
Channel Change Events

This chart displays a time-series graph showing the number of channel change events that occurred for this specific radio.



Channel Change Reason

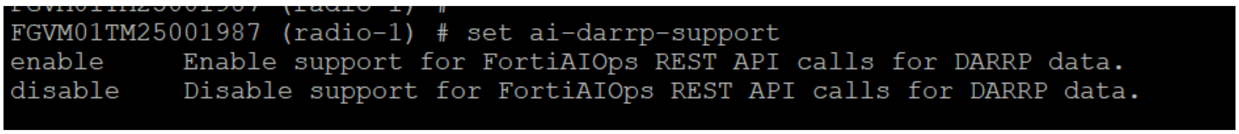
This chart categorizes why the channel change events took place. It identifies the specific trigger for the channel switches such as **High Channel Utilization**, **Noise**, **Co-Channel Interference**, **RF Other**, or **DARRP**.



Disabling AI-ARRP

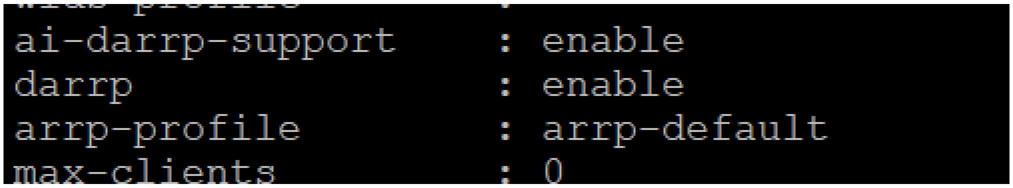
You can disable AI-DARRP support on a per-radio basis using the FortiAP CLI WTP profile. Use the `set ai-darrp-support` command to enable or disable AI-ARRP on any radio.

```
#config wireless-controller wtp-profile
#edit FAP243K-default
# config radio-1
# set ai-darrp-support
enable Enable support for FortiAIOps REST API calls for DARRP data.
disable Disable support for FortiAIOps REST API calls for DARRP data.
```



```
FGVM01TM25001987 (radio-1) # set ai-darrp-support
enable      Enable support for FortiAIOps REST API calls for DARRP data.
disable     Disable support for FortiAIOps REST API calls for DARRP data.
```

Note: For AI-DARRP to function correctly, both `darrp` and `ai-darrp-support` must be enabled in the WTP profile.



```
ai-darrp-support        : enable
darrp                   : enable
arrp-profile            : arrp-default
max-clients             : 0
```

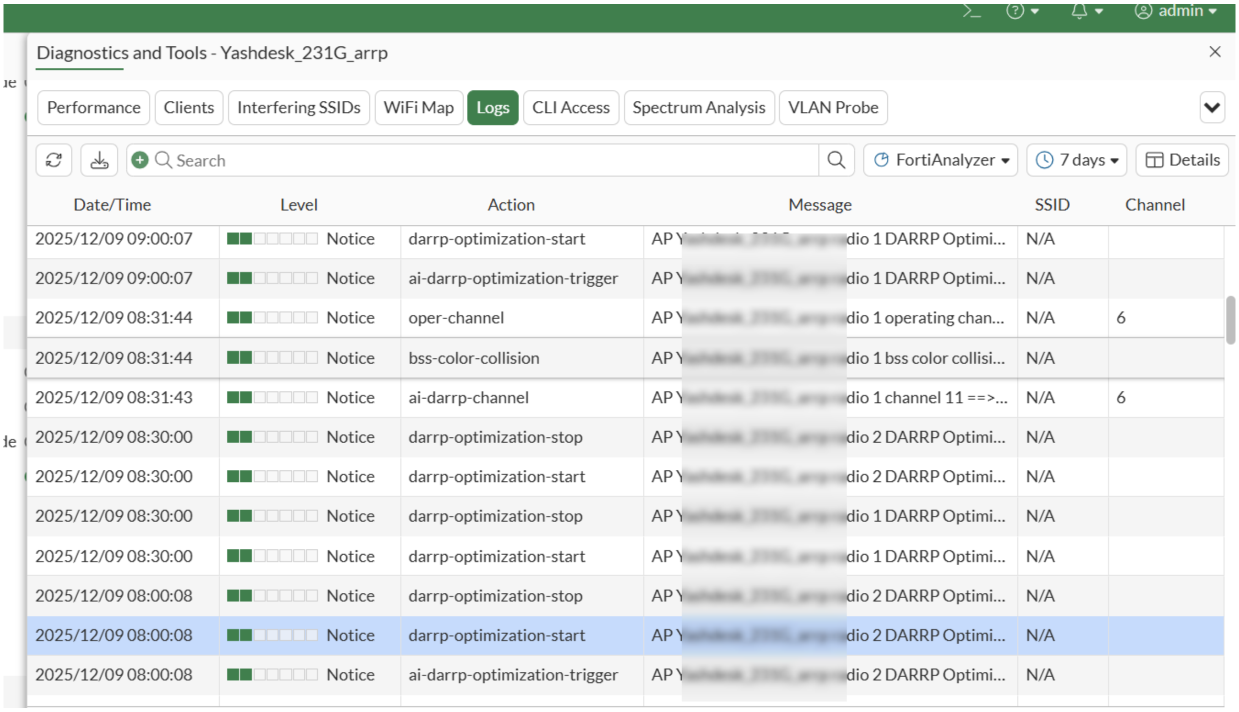
Logging and Diagnostics

AI-ARRP generates detailed logs during scheduled DARRP operations to track channel planning and execution.

The Local Logs section displays two primary event types:

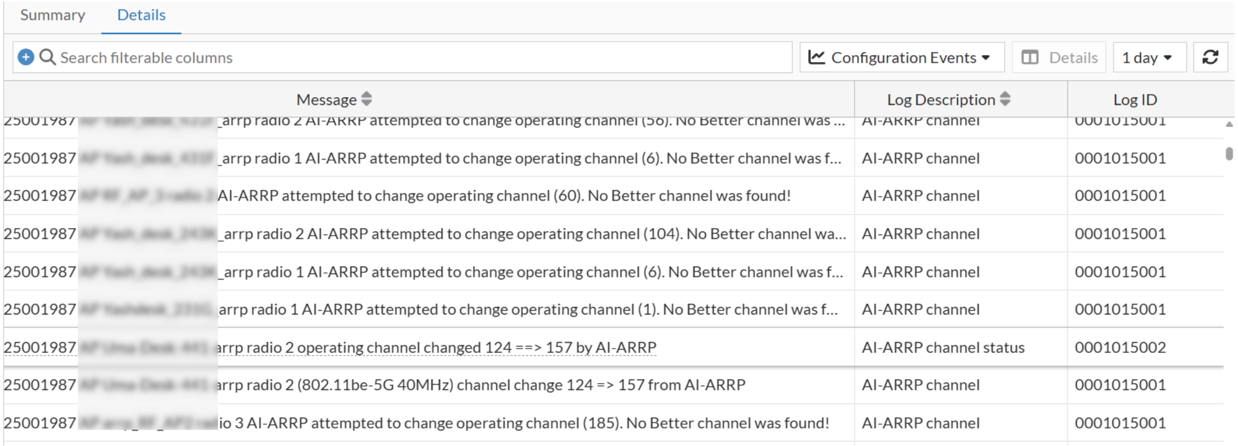
- AI-ARRP Channel: Generated whenever a new channel is suggested or an existing channel is retained for an AP radio.
- AI-ARRP Channel Status: Indicates whether the channel change initiated on the FortiGate was successful or failed.

FortiGate Logs Related logs can be viewed on the FortiGate under **Diagnostics** > **Logs**.



Date/Time	Level	Action	Message	SSID	Channel
2025/12/09 09:00:07	Notice	darrp-optimization-start	AP Y[redacted]dio 1 DARRP Optimi...	N/A	
2025/12/09 09:00:07	Notice	ai-darrp-optimization-trigger	AP Y[redacted]dio 1 DARRP Optimi...	N/A	
2025/12/09 08:31:44	Notice	oper-channel	AP Y[redacted]dio 1 operating chan...	N/A	6
2025/12/09 08:31:44	Notice	bss-color-collision	AP Y[redacted]dio 1 bss color collisi...	N/A	
2025/12/09 08:31:43	Notice	ai-darrp-channel	AP Y[redacted]dio 1 channel 11 ==>...	N/A	6
2025/12/09 08:30:00	Notice	darrp-optimization-stop	AP Y[redacted]dio 2 DARRP Optimi...	N/A	
2025/12/09 08:30:00	Notice	darrp-optimization-start	AP Y[redacted]dio 2 DARRP Optimi...	N/A	
2025/12/09 08:30:00	Notice	darrp-optimization-stop	AP Y[redacted]dio 1 DARRP Optimi...	N/A	
2025/12/09 08:30:00	Notice	darrp-optimization-start	AP Y[redacted]dio 1 DARRP Optimi...	N/A	
2025/12/09 08:00:08	Notice	darrp-optimization-stop	AP Y[redacted]dio 2 DARRP Optimi...	N/A	
2025/12/09 08:00:08	Notice	darrp-optimization-start	AP Y[redacted]dio 2 DARRP Optimi...	N/A	
2025/12/09 08:00:08	Notice	ai-darrp-optimization-trigger	AP Y[redacted]dio 2 DARRP Optimi...	N/A	

For granular details regarding channel validations, refer to the `aiarrp_report.log` file located in the FortiAIOps diagnostics section.



Message	Log Description	Log ID
25001987 [redacted] _arrp radio 2 AI-ARRP attempted to change operating channel (56). No Better channel was ...	AI-ARRP channel	0001015001
25001987 [redacted] _arrp radio 1 AI-ARRP attempted to change operating channel (6). No Better channel was f...	AI-ARRP channel	0001015001
25001987 [redacted] AI-ARRP attempted to change operating channel (60). No Better channel was found!	AI-ARRP channel	0001015001
25001987 [redacted] _arrp radio 2 AI-ARRP attempted to change operating channel (104). No Better channel wa...	AI-ARRP channel	0001015001
25001987 [redacted] _arrp radio 1 AI-ARRP attempted to change operating channel (6). No Better channel was f...	AI-ARRP channel	0001015001
25001987 [redacted] arrp radio 1 AI-ARRP attempted to change operating channel (1). No Better channel was f...	AI-ARRP channel	0001015001
25001987 [redacted] arrp radio 2 operating channel changed 124 ==> 157 by AI-ARRP	AI-ARRP channel status	0001015002
25001987 [redacted] arrp radio 2 (802.11be-5G 40MHz) channel change 124 => 157 from AI-ARRP	AI-ARRP channel	0001015001
25001987 [redacted] io 3 AI-ARRP attempted to change operating channel (185). No Better channel was found!	AI-ARRP channel	0001015001

Enhanced Wi-Fi Maps

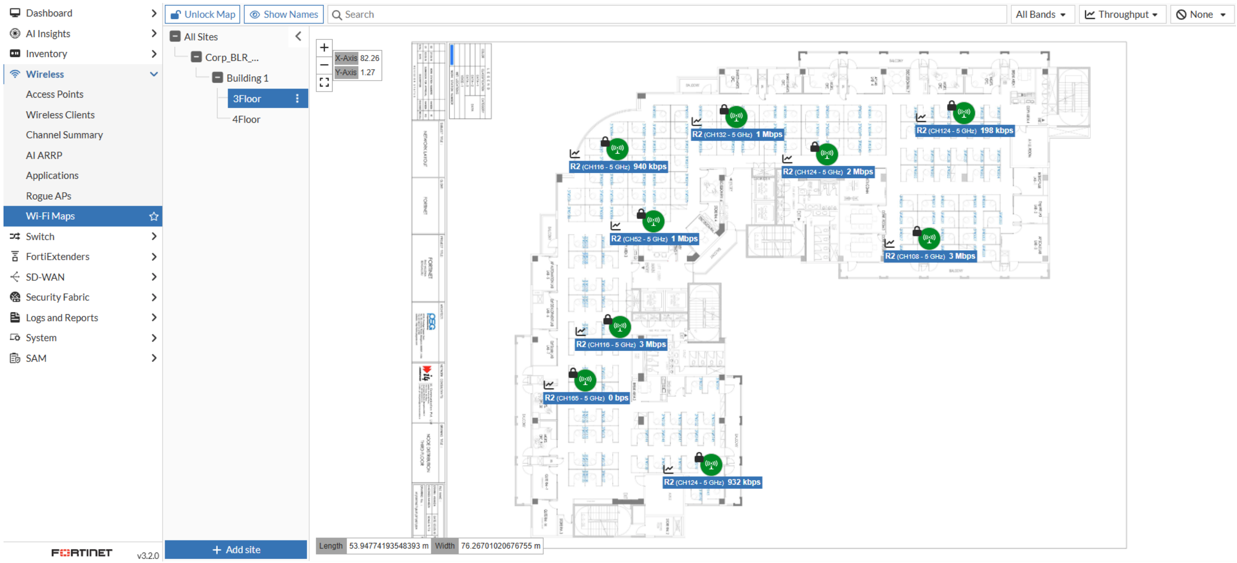
This release significantly upgrades the map feature, now rebranded as **Wi-Fi Maps**, delivering enhanced functionality, a modernized user interface, and improved compatibility for seamless real-time monitoring.

The new standardized GUI aligns the look and feel with other Fortinet products, ensuring a consistent user experience. **Wi-Fi Maps** is now compatible with **Ekahau**, a leading Wi-Fi planning tool. You can easily export and import .esx files to modify maps by adding sites, buildings, floors, and AP locations, and then export the updated map back to Ekahau for live survey operations. The map provides real-time status and alerts for your FortiAPs, allowing for quick visualization of each unit on custom uploaded floor plans.

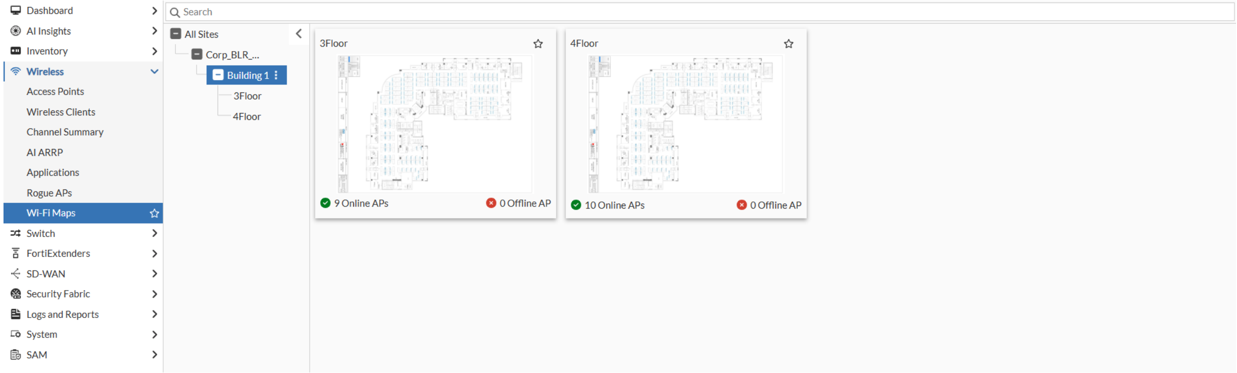
This is complemented by an enhanced **Locate** feature available across the wireless management screens, enabling you to immediately pinpoint the physical location of any Access Point or wireless client directly on your maps.

After upgrading to Release 3.2.0:

- All valid floor maps will be successfully migrated to the new **Wi-Fi Maps** feature.
- All existing AP placements and their configured features will be fully retained and carried over to the new system.



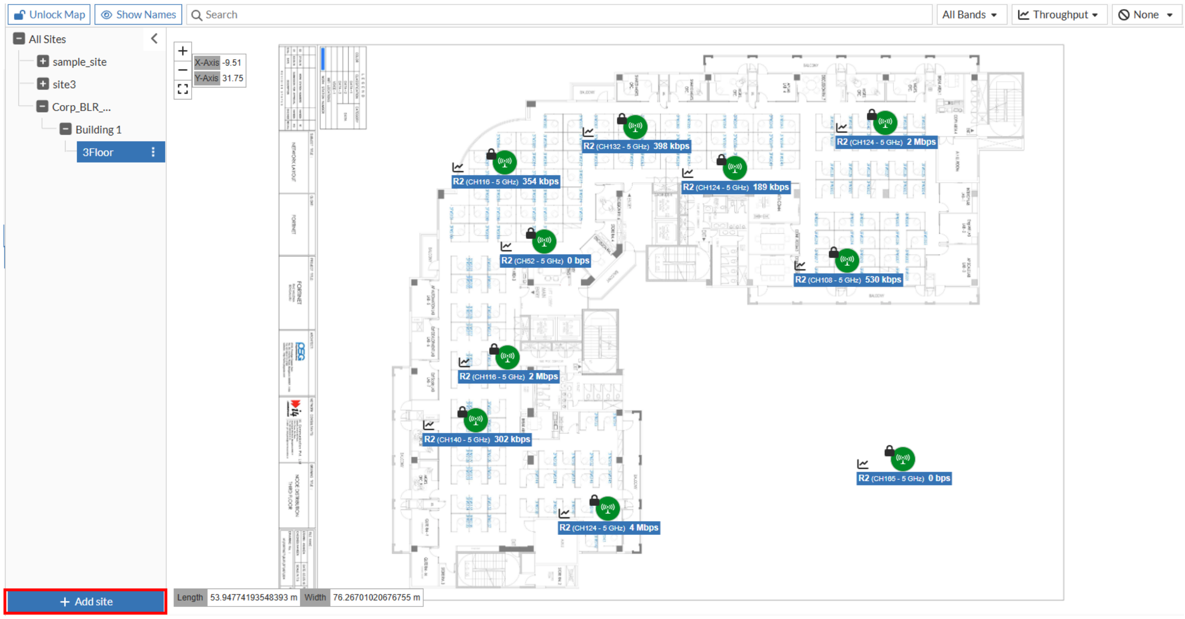
The map structure is organized hierarchically, starting with the largest entity: **Site** > **Building** > **Floor**.



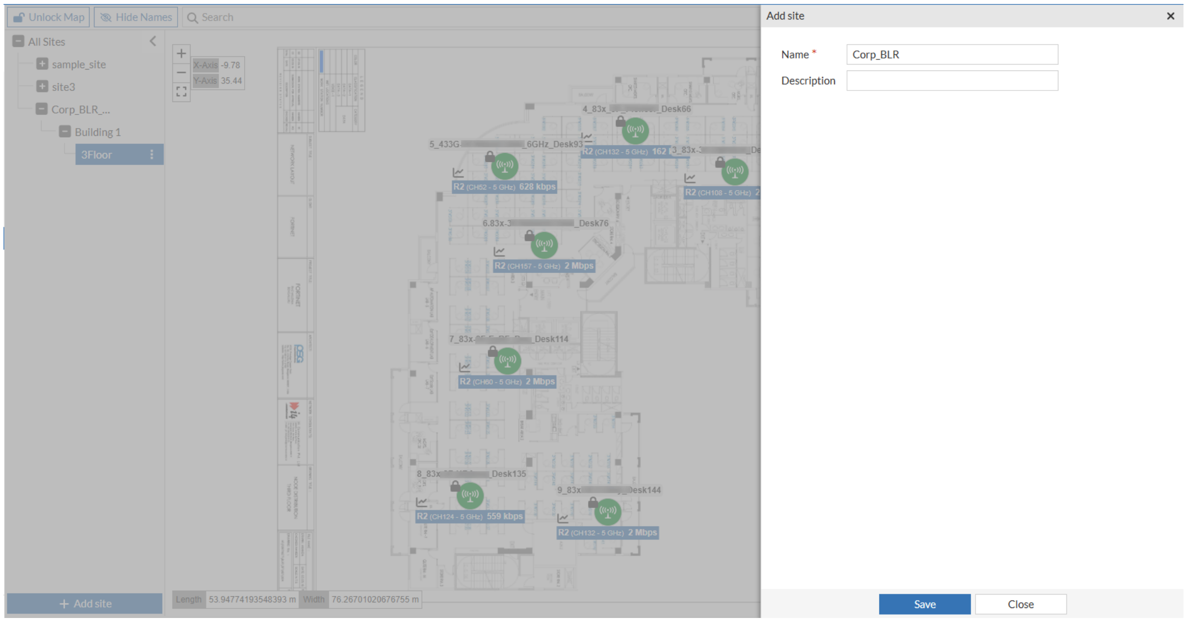
Adding a Site

A site is the top-level entity that contains multiple buildings.

1. Navigate to **Wireless** > **Wi-Fi Maps**.
2. Click **Add site**.


Unlock Map
Show Names
Search
All Bands
Throughput
None
All Sites
sample_site
site3
Corp_BLR_...
Building 1
3Floor
X-Axis -9.51
Y-Axis 31.75
R2 (CH132 - 5 GHz) 398 kbps
R2 (CH124 - 5 GHz) 2 Mbps
R2 (CH116 - 5 GHz) 354 kbps
R2 (CH124 - 5 GHz) 189 kbps
R2 (CH52 - 5 GHz) 0 bps
R2 (CH108 - 5 GHz) 530 kbps
R2 (CH116 - 5 GHz) 2 Mbps
R2 (CH140 - 5 GHz) 302 kbps
R2 (CH165 - 5 GHz) 0 bps
R2 (CH124 - 5 GHz) 4 Mbps
+ Add site
Length 53.94774193548393 m
Width 76.26701020676755 m

3. In the **Add site** pane, enter a **Name** and a **Description**.



Add site

Name * Corp_BLR

Description

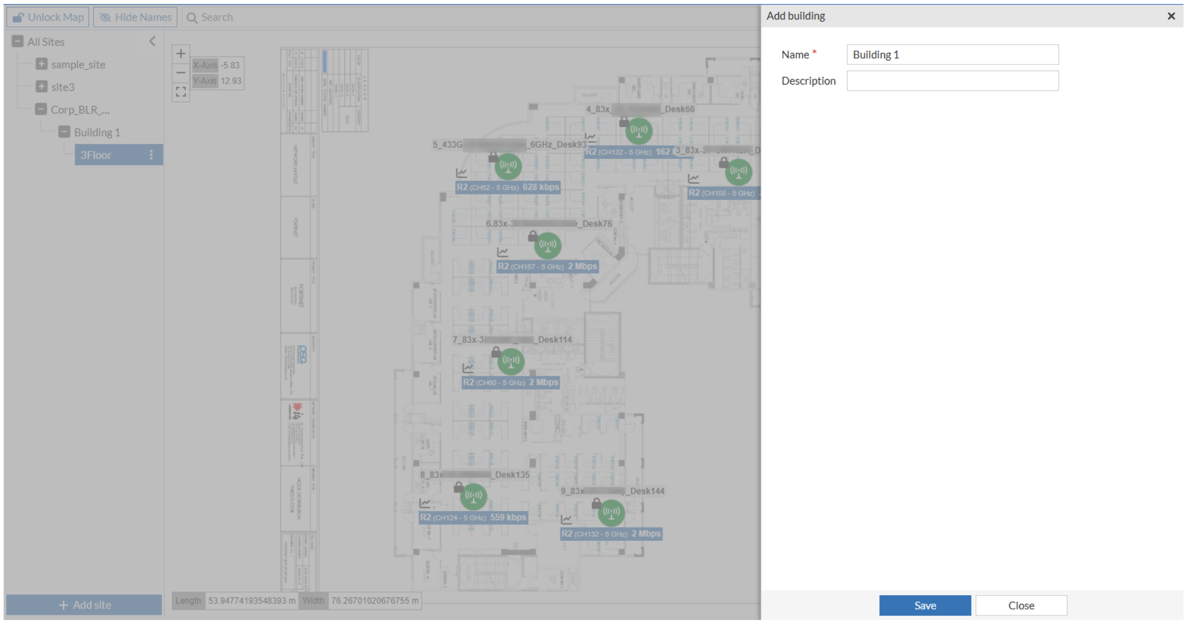
4. Click **Save**. The new site will appear in the left pane under **All Sites**.

Note: To delete a site, click the Kebob menu (vertical ellipsis) next to the site and click **Delete**. Deleting a site will delete the entire hierarchy contained within that site.

Adding a Building

A building is contained within a site and can have multiple floors.

1. On the left pane, select the site where you want to add a building.
2. Click the Kebob menu (vertical ellipsis) next to the site and click **Add Building**.



Add building

Name * Building 1

Description

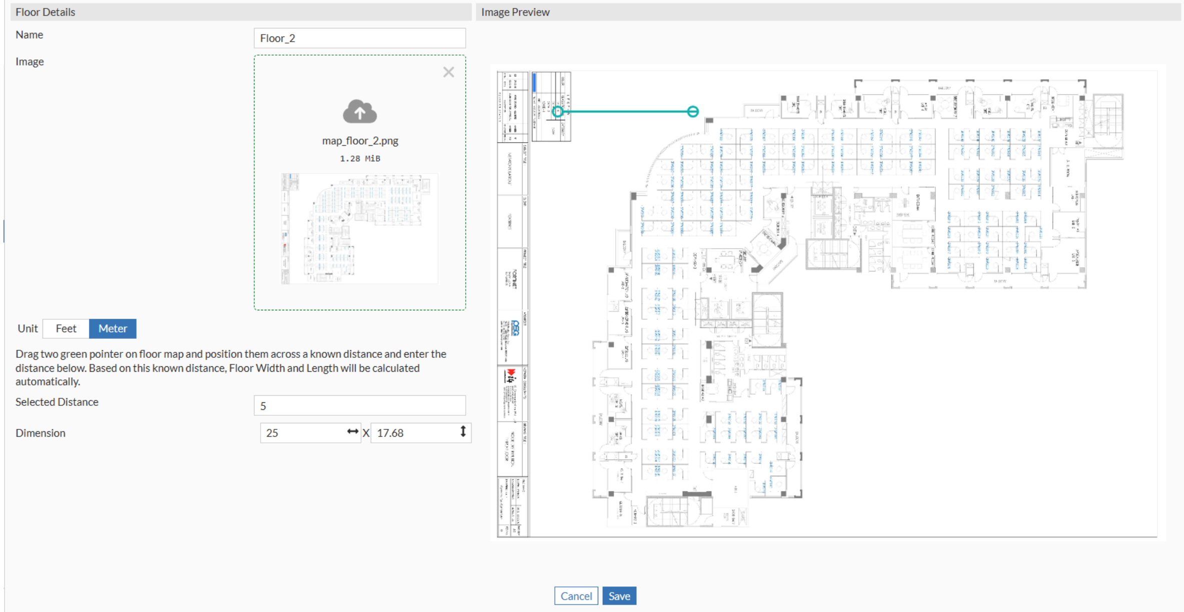
3. On the **Add building** pane, enter a **Name** and **Description**.
4. Click **Save**. The new building will appear under the selected site in the left pane.

Note: To delete a building, click the Kebob menu (vertical ellipsis) next to the site and click **Delete.** Deleting a building will delete the entire hierarchy contained within that building.

Adding a Floor

A floor is contained within a building and requires uploading a map image.

1. On the left pane, select the site and the building where you want to add a floor.
2. Click the Kebob menu (vertical ellipsis) next to the building and click **Add Floor**.
3. In the Floor Details section, enter a Name for the floor.
4. Upload the floor map file (must be in .jpg, .png, or .jpeg format).



Floor Details

Name: Floor_2

Image: map_floor_2.png 1.28 MiB

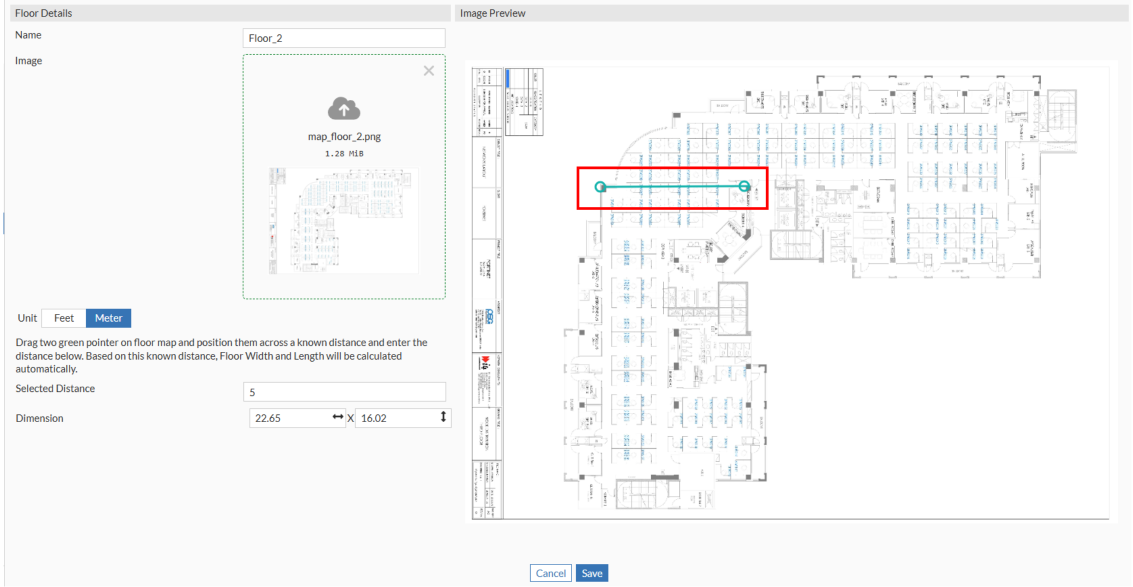
Unit: Feet | Meter

Drag two green pointer on floor map and position them across a known distance and enter the distance below. Based on this known distance, Floor Width and Length will be calculated automatically.

Selected Distance: 5

Dimension: 25 ↔ X 17.68 ↕

5. Set the map scale:
   a. In the **Image Preview section**, drag the green pointer to two points on the map with a known distance between them.



Floor Details

Name: Floor_2

Image: map_floor_2.png 1.28 MiB

Unit: Feet | Meter

Drag two green pointer on floor map and position them across a known distance and enter the distance below. Based on this known distance, Floor Width and Length will be calculated automatically.

Selected Distance: 5

Dimension: 22.65 ↔ X 16.02 ↕

b. Under **Floor Details**, specify the **Unit** of measurement.
c. Enter the actual distance between the two selected points in the **Selected Distance** field. The system automatically computes and displays the correct map scale in the **Dimension** field.
d. Click **Save**. The new floor will appear under the selected site in the left pane.

Note: To delete a floor, click the Kebob menu (vertical ellipsis) next to the floor and click **Delete**. Deleting a floor will delete the entire hierarchy contained within that floor.

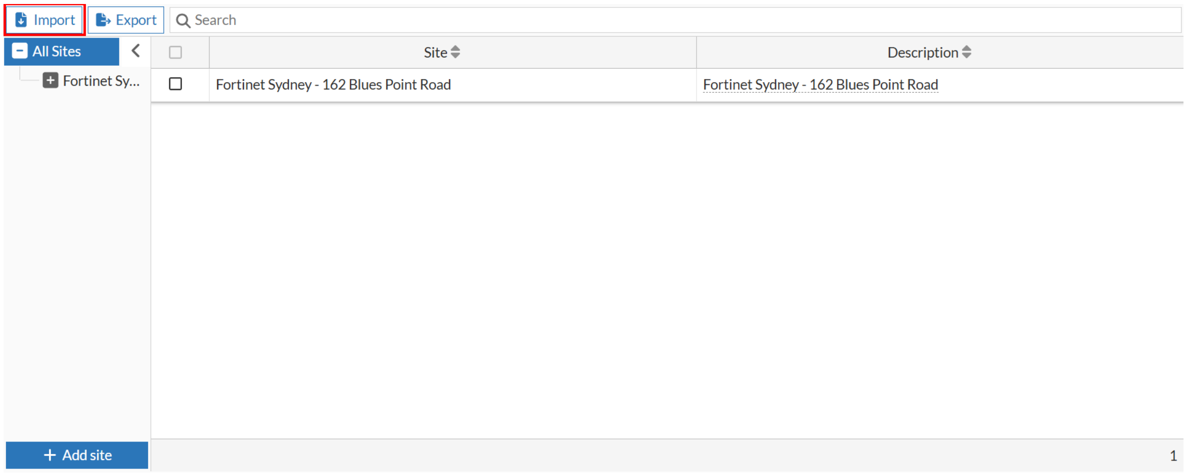
Importing and Exporting Maps

You can now exchange Wi-Fi maps with **Ekahau**, allowing you to import new maps and export modified ones for deeper analysis in the **Ekahau** application.

Importing Maps

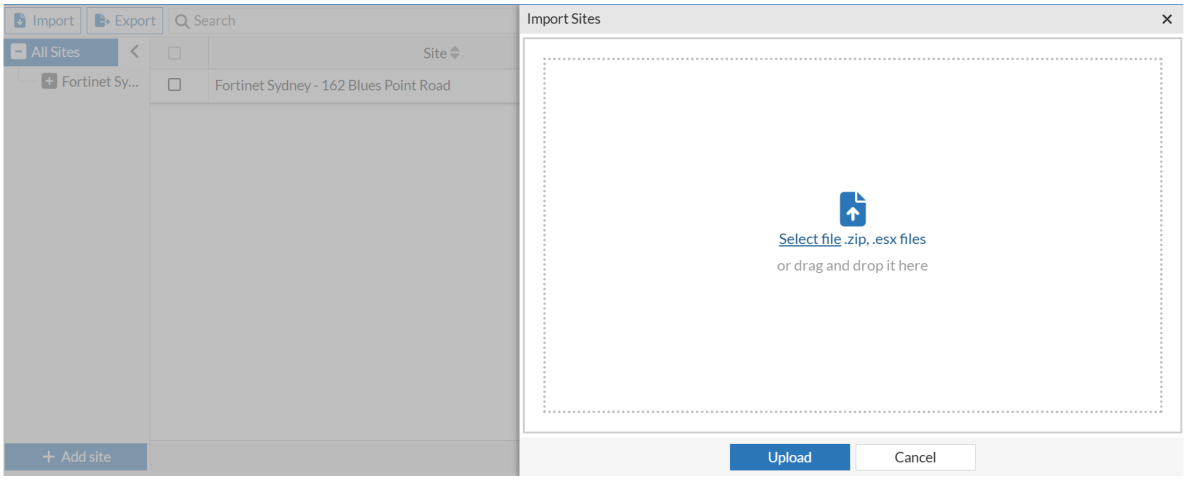
You can import maps created or modified in **Ekahau** directly into the system:

1. Navigate to **Wireless** > **Wi-Fi Maps**.
2. In the left pane, select **All Sites** or any site to import maps. Click **Import**.
   Note: Maximum supported .zip or .esx file is 250 MB.



☐	Site	Description
☐	Fortinet Sydney - 162 Blues Point Road	Fortinet Sydney - 162 Blues Point Road

3. In the **Import Sites** pane, select your **Ekahau** file (either a .esx file or a .zip file containing multiple .esx files).



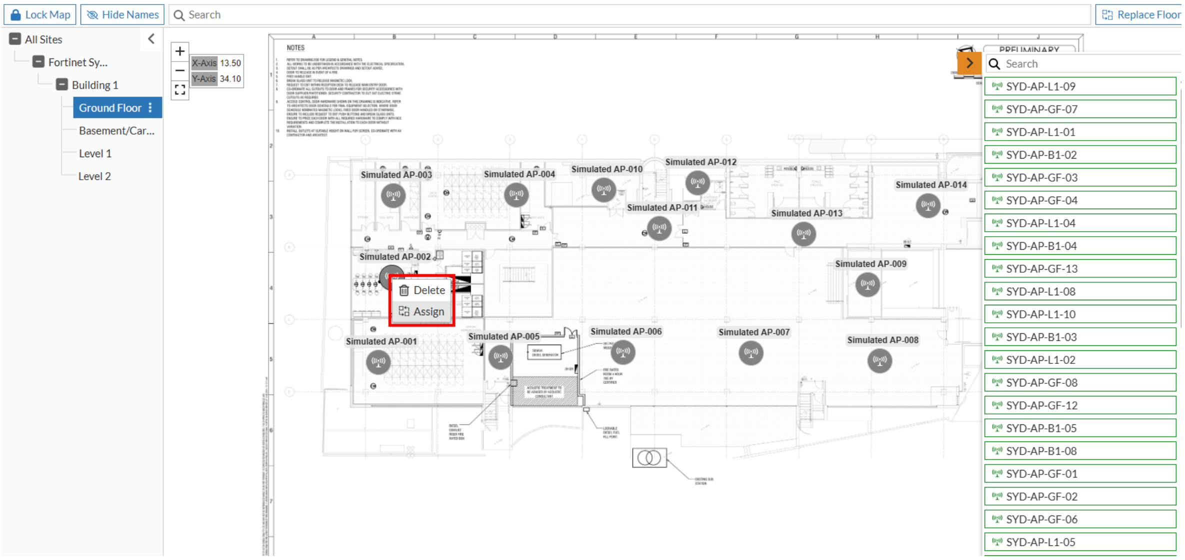
4. Click **Upload**.
   The imported maps will appear in the left pane, structured appropriately.

Mapping APs

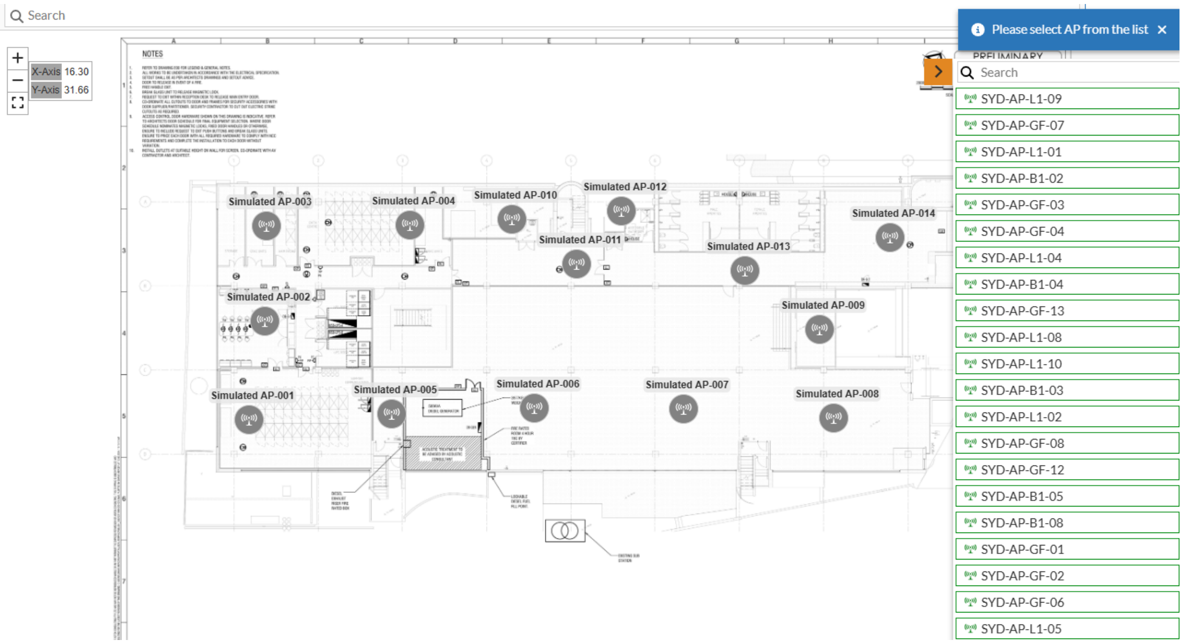
If the Access Point (AP) names in the imported map match your existing inventory names, the APs are mapped to their floor plan locations automatically.

If AP names do not match, those APs will be displayed in an **Inactive** state. To map them:

1. Click **Unlock Map**.
2. Select the unplaced AP on the map. Click **Assign**.



3. A list of unplaced APs will appear; select the correct AP from this list to assign it to the selected location.

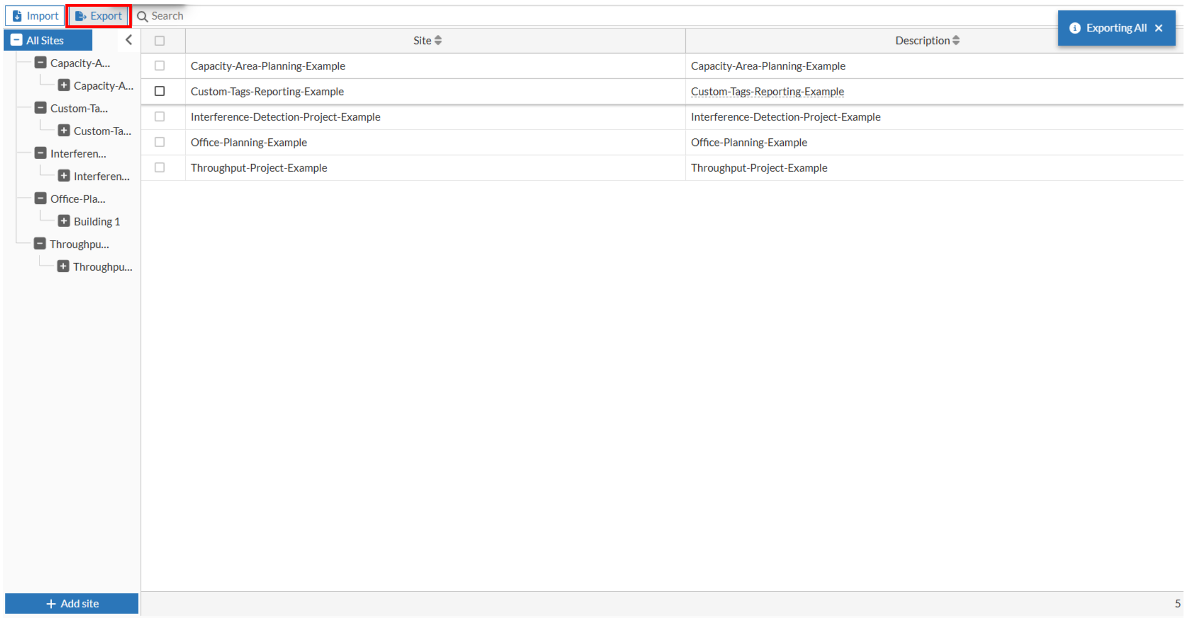


4. Click **Lock Map** when finished.

Exporting Maps

You can export modified maps and use them in Ekahau for further analysis.

1. Navigate to **Wireless** > **Wi-Fi Maps**.
2. To export all sites, select **All Sites**.
3. To export specific sites, use the check boxes to select the individual ones.



☐	Site	Description
☐	Capacity-Area-Planning-Example	Capacity-Area-Planning-Example
☐	Custom-Tags-Reporting-Example	Custom-Tags-Reporting-Example
☐	Interference-Detection-Project-Example	Interference-Detection-Project-Example
☐	Office-Planning-Example	Office-Planning-Example
☐	Throughput-Project-Example	Throughput-Project-Example

4. To export specific sites, use the check boxes to select the individual sites or navigate to the site (in the hierarchy) and click **Export**.
   A .zip file containing the map(s) will be downloaded.

Modifying the Map

The **Unlock Map**/**Lock Map** options enables you to make any modifications to the floor map that is uploaded. You can make the following changes after you unlock a map:

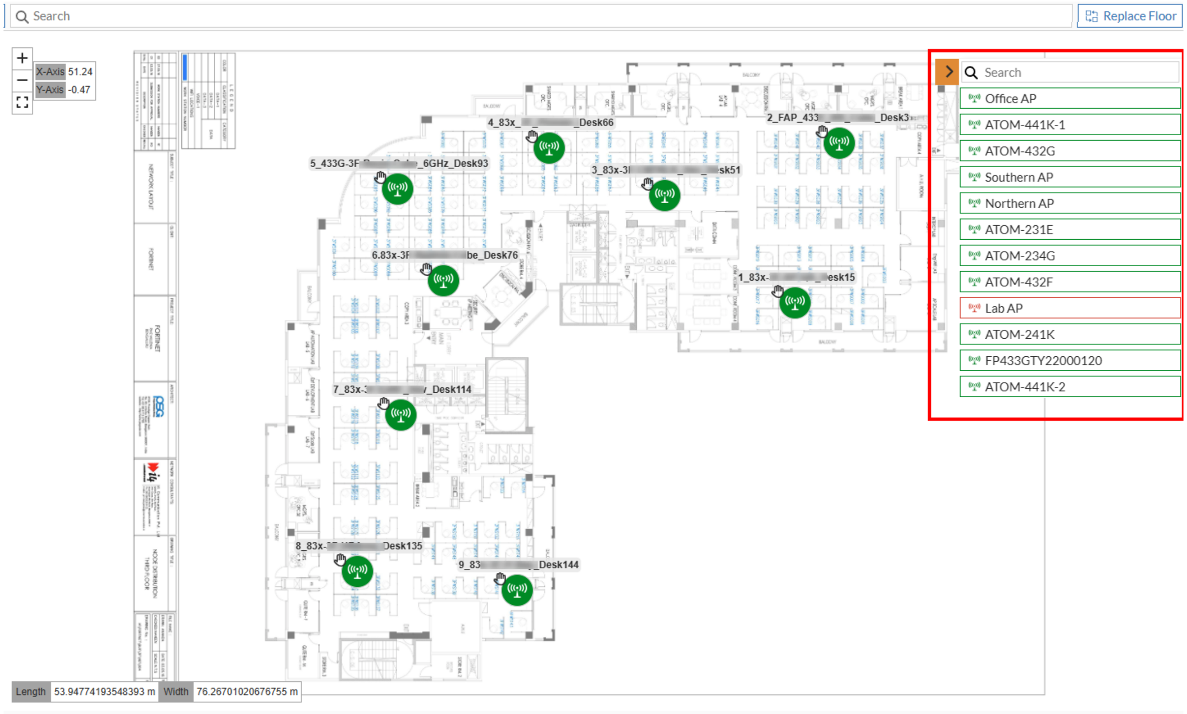
- Placing an Access Point – when you unlock a map, the available APs are listed that can be placed on the map.
- Replacing an Access Point – replace an AP that is already added to a map with a different one.
- Deleting an Access Point – delete an AP that is added to the map.
- Replacing a Floor Map – replace the existing floor map with a different one.

Use the **Lock Map** option to save any changes made to the map during the **Unlock Map** phase.

Placing an Access Point

To place an AP on the floor map:

1. Navigate to the floor map and click **Unlock Map**.
2. On the right pane, a list of APs that are not placed is displayed.



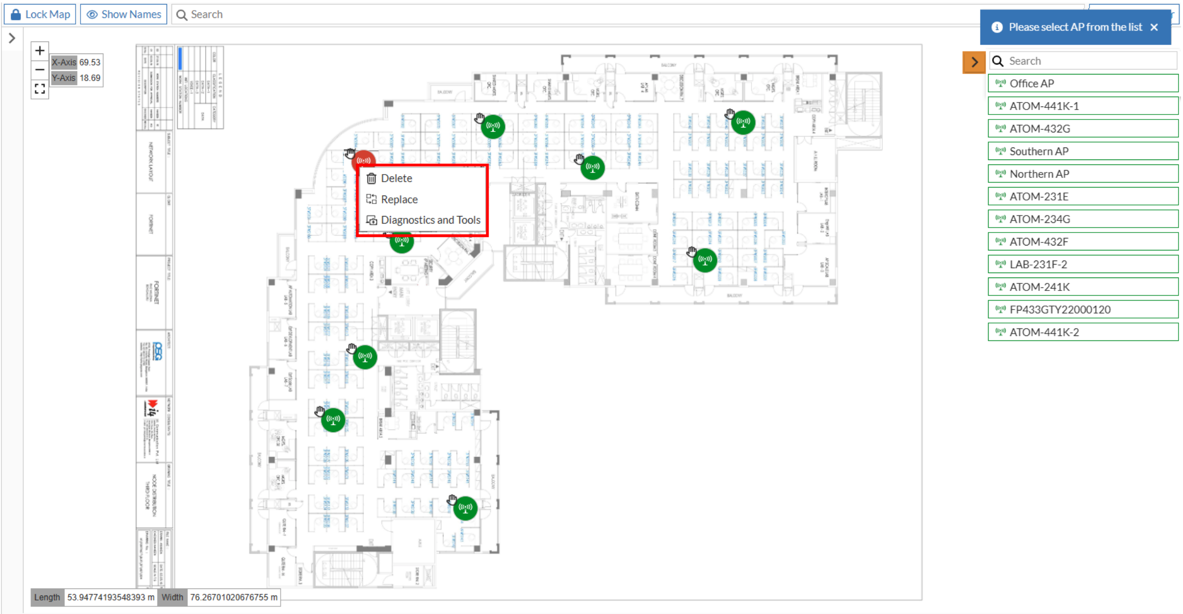
3. Drag and drop an AP at the desired location on the map.
4. Click **Lock Map** to save the changes.

Replacing an Access Point

To replace an existing AP with a different one on the floor map:

1. Navigate to the floor map and click **Unlock Map**.
2. On the right pane, a list of APs that are not placed is displayed.

3. Click the AP that you want to replace on the map and select **Replace**.



Please select AP from the list

4. Select the required AP from the list. The AP selected on the map is replaced with the AP selected from the list.
5. Click **Lock Map** to save the changes.

Deleting an Access Point

To delete an AP from a floor map:

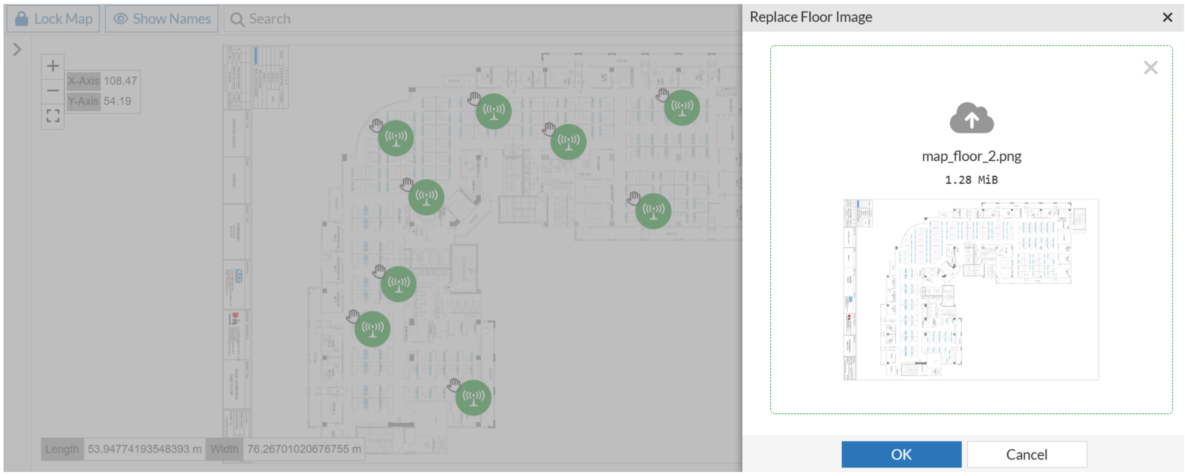
1. Navigate to the floor map and click **Unlock Map**.
2. Click the AP that you want to delete and select **Delete**.
   The deleted AP is displayed on the **Unplaced Device(s)** list and can be re-used as necessary.
3. Click **Lock Map** to save the changes.

Replacing a Floor Map

To replace a floor map:

1. Navigate to the floor map and click **Unlock Map**.
2. Click **Replace Floor**.

3. In the **Replace Floor Image** pane, upload the floor map in either .jpg, .png, or .jpeg format and click **OK**.



X-Axis 108.47
Y-Axis 54.19

Length 53.94774193548393 m
Width 76.26701020676755 m

map_floor_2.png
1.28 MiB

4. Click **Lock Map** to save the changes.

Viewing the Map

AP Status

The status of an AP reflecting its connectivity is displayed on the map:

Online (Green)	The AP is currently active and connected.
Offline (Red)	The AP is currently disconnected or unreachable.
Inactive (Grey)	The AP is displayed on the map but is not actively managed by the current inventory. This state applies if: • The AP belongs to a Deleted FortiGate. • The FortiGate associated with the AP was moved from current ADOM to a different ADOM. • The AP was loaded using an Imported Map and its name does not match the AP names in the current ADOM's Access Point Inventory.

Show/Hide Names

Toggle the Hide Names and Show Names button to hide or display the customized names of the APs placed on the floor map.

Search Bar

The **Wi-Fi Maps** page features a global search bar that enables you to quickly locate devices and navigate through the map hierarchy. The following search types are supported:

- Site, Building, or Floor.
- AP Name or Serial Number.
- Device Name or Client MAC Address.

When a match is found, the map automatically navigates to the corresponding site, building, or floor and highlights the associated AP or client. This facilitates quick device location, placement review, and connectivity troubleshooting.

If the search query does not immediately match a known Site, Building, or Floor, the system displays a prompt allowing you to refine the scope:

- Search for Client: Scans for connected clients by MAC address or device name, then navigates to the floor where the client is currently associated.
- Search for AP: Scans for APs by name or serial number and highlights them on the map.

Selecting one of these options restricts the search to the chosen category and displays the relevant results.

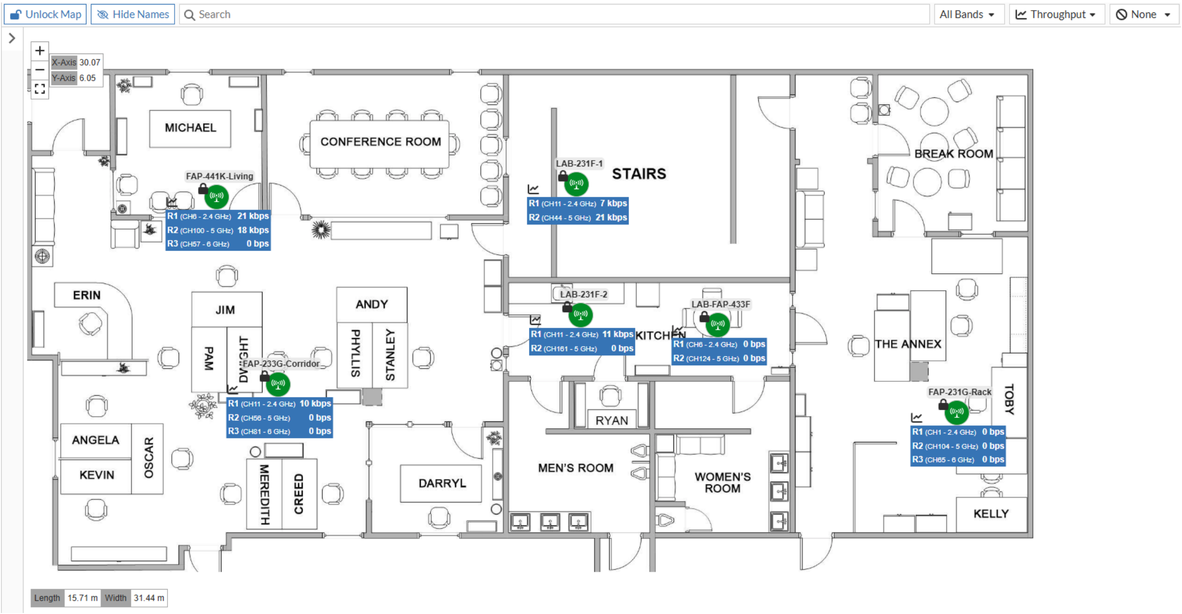
Bands

Bands filter the AP stats and Heatmaps data based on the specific band for the APs in the Inventory. This helps to visualize the AP distribution per frequency band.

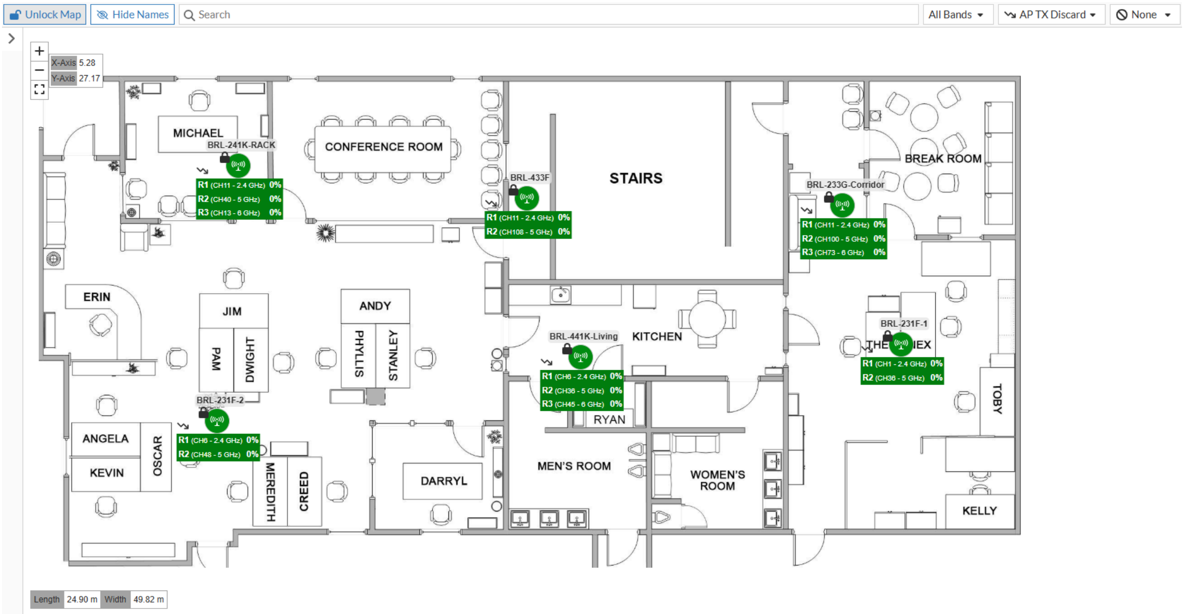
AP Stats

Select from the AP Stats drop-down menu to display real-time statistical data on the map for each AP. Available options include:

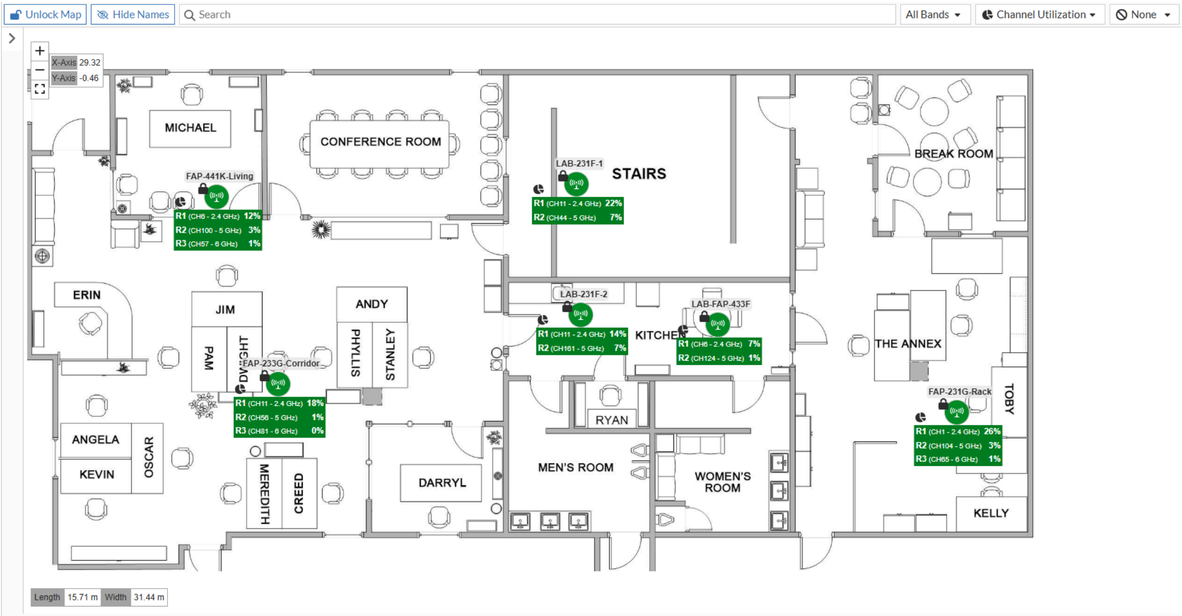
- Throughput



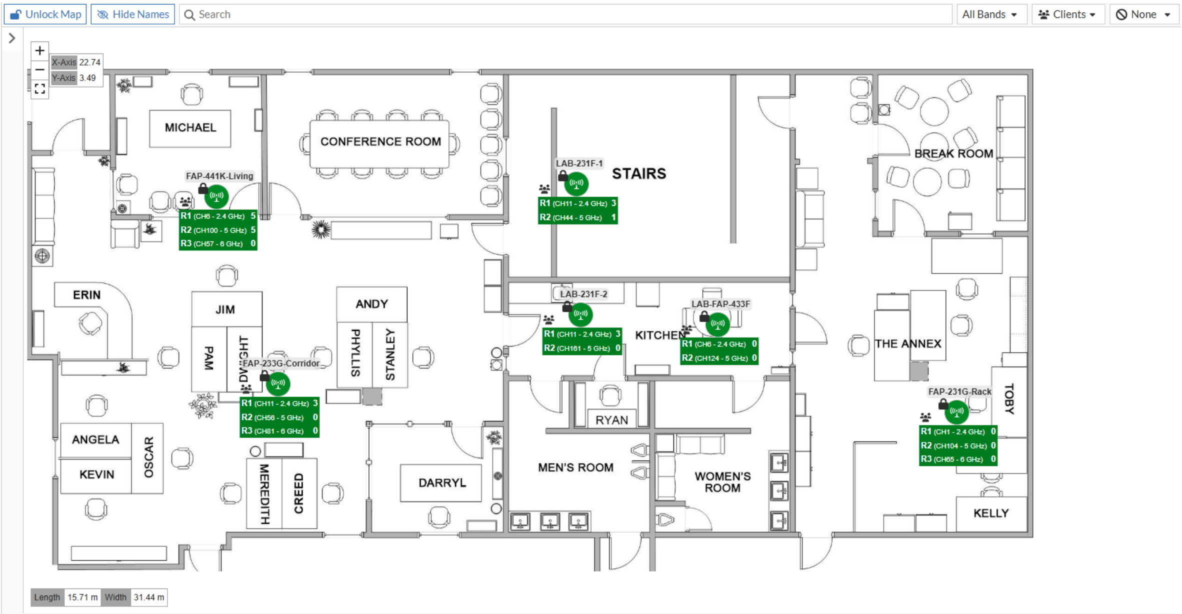
- AP TX Discard



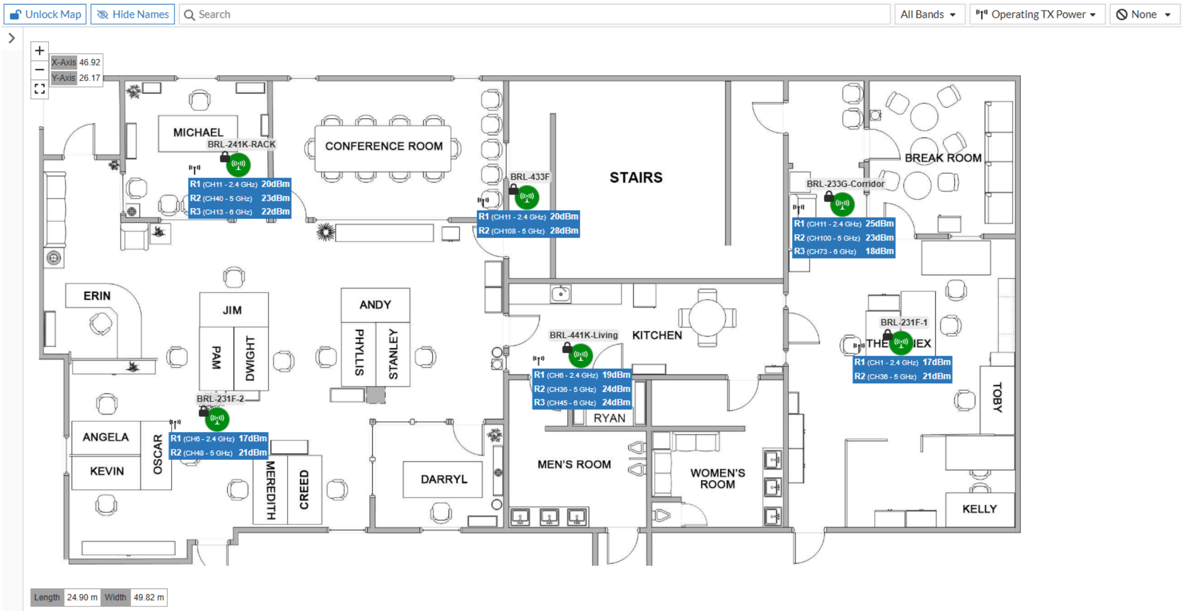
- Channel Utilization



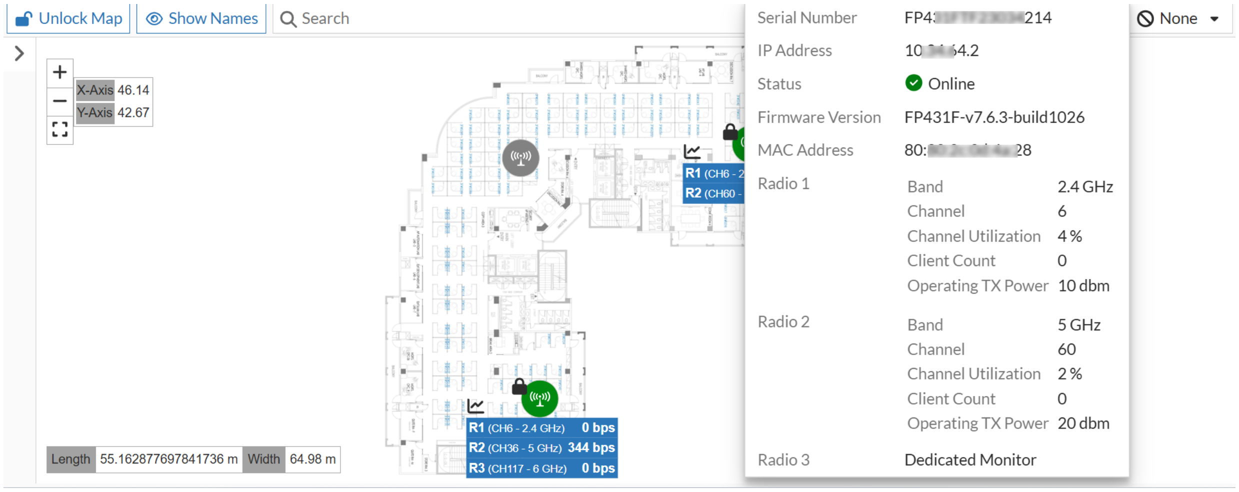
- Clients



- Operating TX Power



Hover over the AP to view more details.



Serial Number	FP4[redacted]214		
IP Address	10[redacted]4.2		
Status	✓ Online		
Firmware Version	FP431F-v7.6.3-build1026		
MAC Address	80:[redacted]28		
Radio 1		Band	2.4 GHz
		Channel	6
		Channel Utilization	4 %
		Client Count	0
		Operating TX Power	10 dbm
Radio 2		Band	5 GHz
		Channel	60
		Channel Utilization	2 %
		Client Count	0
		Operating TX Power	20 dbm
Radio 3	Dedicated Monitor		

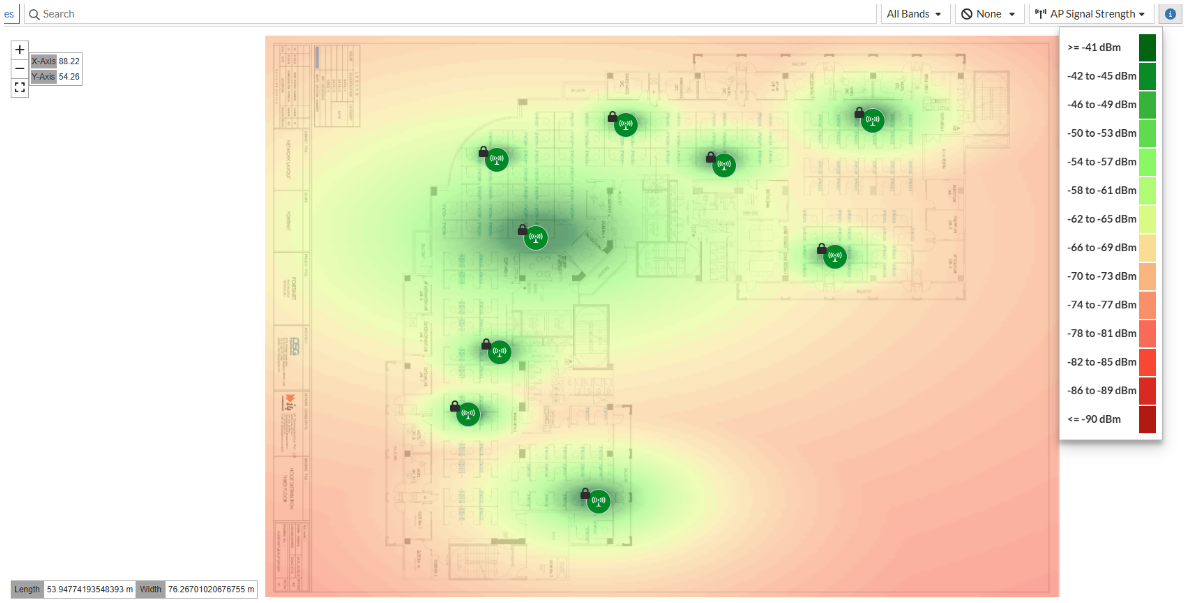
R1 (CH6 - 2.4 GHz)	0 bps
R2 (CH36 - 5 GHz)	344 bps
R3 (CH117 - 6 GHz)	0 bps

Length 55.162877697841736 m Width 64.98 m

Heatmaps

Select a value from the Heatmaps drop-down to visualize different metrics across the floor map using a color-coded representation (heatmap). Available heatmap values include:

- AP Signal Strength

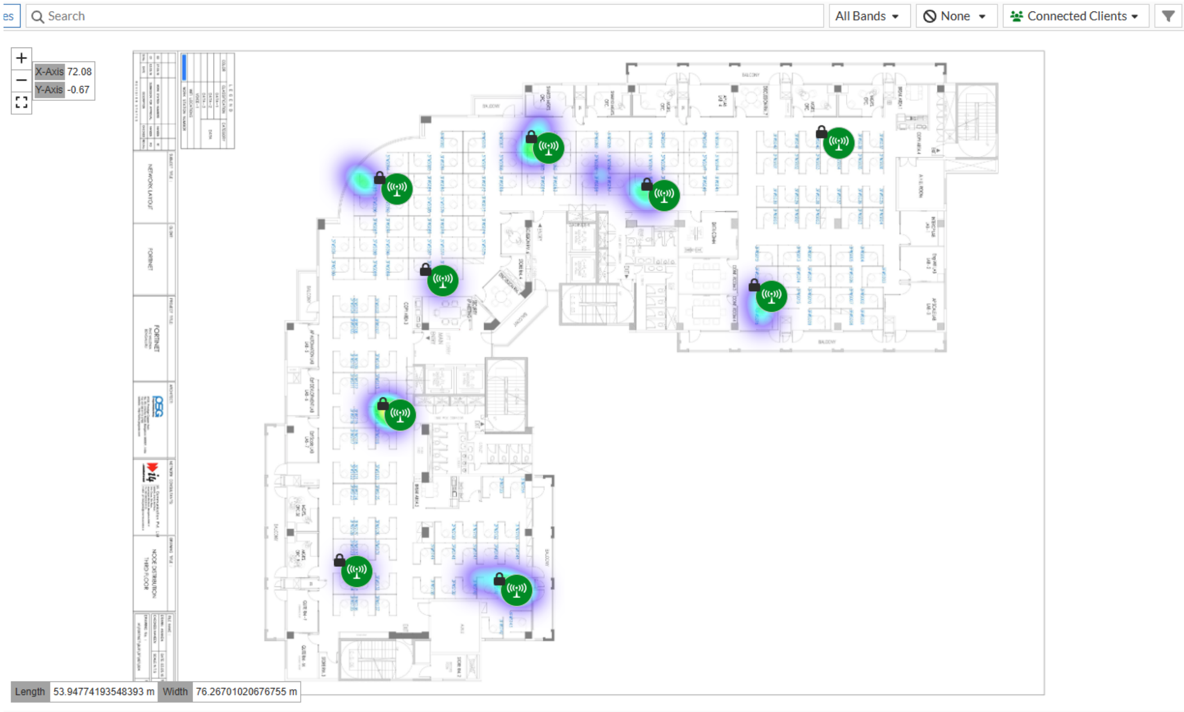


>= -41 dBm	🟩
-42 to -45 dBm	🟩
-46 to -49 dBm	🟩
-50 to -53 dBm	🟩
-54 to -57 dBm	🟩
-58 to -61 dBm	🟩
-62 to -65 dBm	🟨
-66 to -69 dBm	🟨
-70 to -73 dBm	🟧
-74 to -77 dBm	🟧
-78 to -81 dBm	🟥
-82 to -85 dBm	🟥
-86 to -89 dBm	🟥
<= -90 dBm	🟥

Length 53.94774193548393 m Width 76.26701020676755 m

Hover over the ⓘ icon to see the legend explaining the colors used in the heatmap.

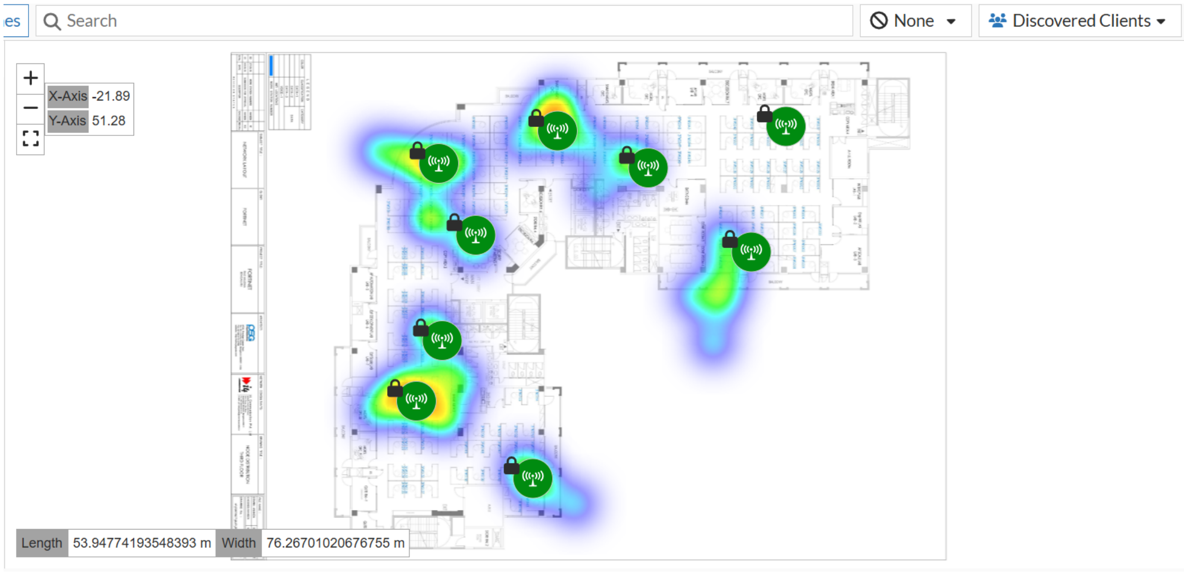
- Connected Clients



X-Axis 72.08
Y-Axis -0.67
Length 53.94774193548393 m
Width 76.26701020676755 m

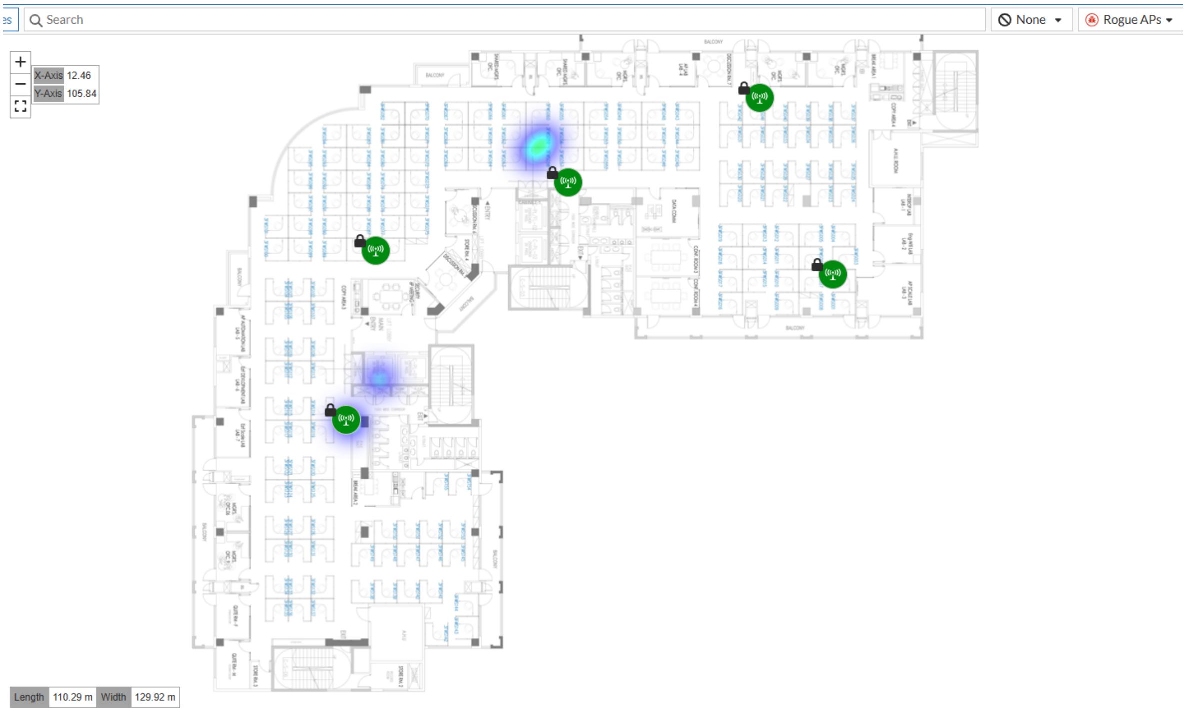
Click the **Filter** button to open the **Advanced Filters** pane. Use the options to narrow the list of connected clients. You can refine your search using the **Accuracy**, **OS Type**, and **Wireless Type** drop-down menus.

- Discovered Clients



X-Axis -21.89
Y-Axis 51.28
Length 53.94774193548393 m
Width 76.26701020676755 m

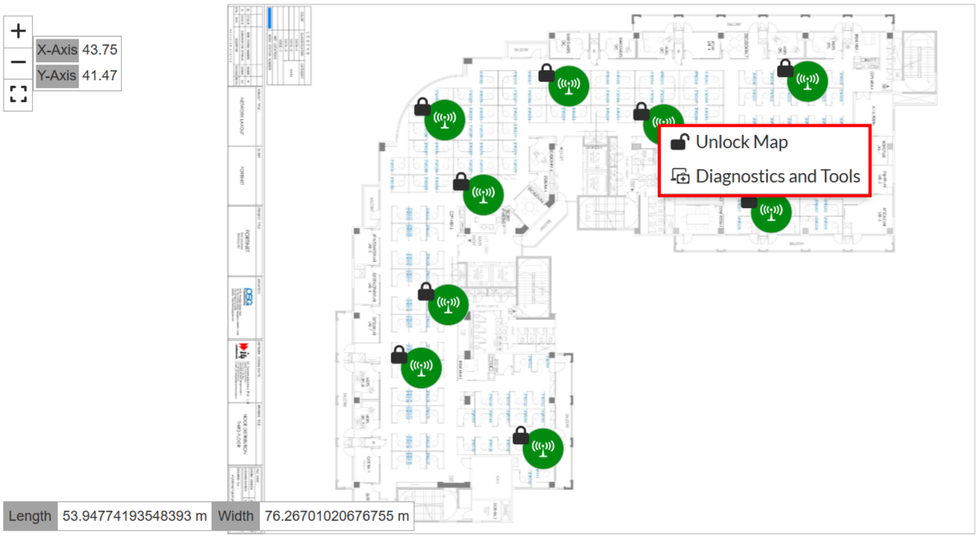
- Rogue APs



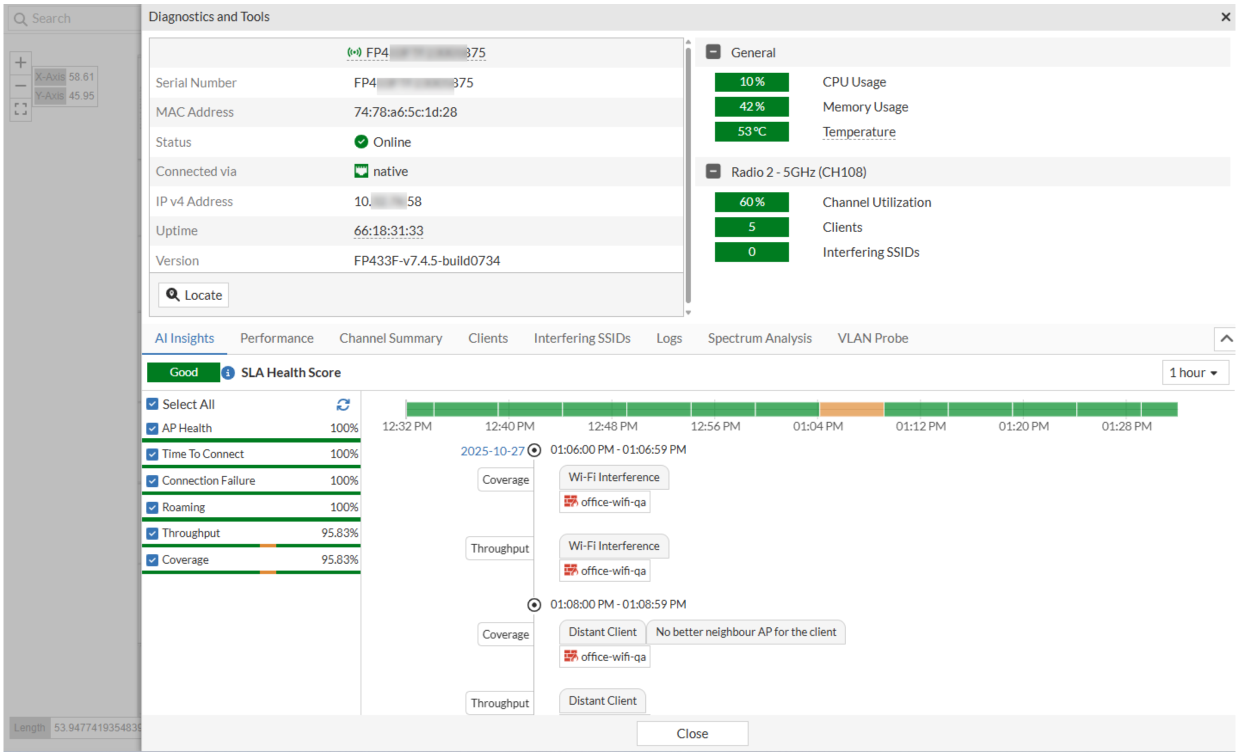
Diagnostics and Tools

The **Diagnostics and Tools** window provides detailed status information and allows you to run diagnostic tests for a selected Access Point. For information, see Access Points Diagnostics and Tools.

To access the **Diagnostics and Tools** window, click on the required Access Point on the map and select **Diagnostics and Tools** from the options displayed.



The **Diagnostics and Tools** pane is displayed.



FP4[redacted]375

Serial Number	FP4[redacted]375
MAC Address	74:78:a6:5c:1d:28
Status	Online
Connected via	native
IP v4 Address	10.[redacted]58
Uptime	66:18:31:33
Version	FP433F-v7.4.5-build0734

General

10 %	CPU Usage
42 %	Memory Usage
53 °C	Temperature

Radio 2 - 5GHz (CH108)

60 %	Channel Utilization
5	Clients
0	Interfering SSIDs

Good SLA Health Score

☑ Select All	
☑ AP Health	100%
☑ Time To Connect	100%
☑ Connection Failure	100%
☑ Roaming	100%
☑ Throughput	95.83%
☑ Coverage	95.83%

12:32 PM 12:40 PM 12:48 PM 12:56 PM 01:04 PM 01:12 PM 01:20 PM 01:28 PM

2025-10-27 01:06:00 PM - 01:06:59 PM
Coverage: Wi-Fi Interference; office-wifi-qa
Throughput: Wi-Fi Interference; office-wifi-qa

01:08:00 PM - 01:08:59 PM
Coverage: Distant Client; No better neighbour AP for the client; office-wifi-qa
Throughput: Distant Client

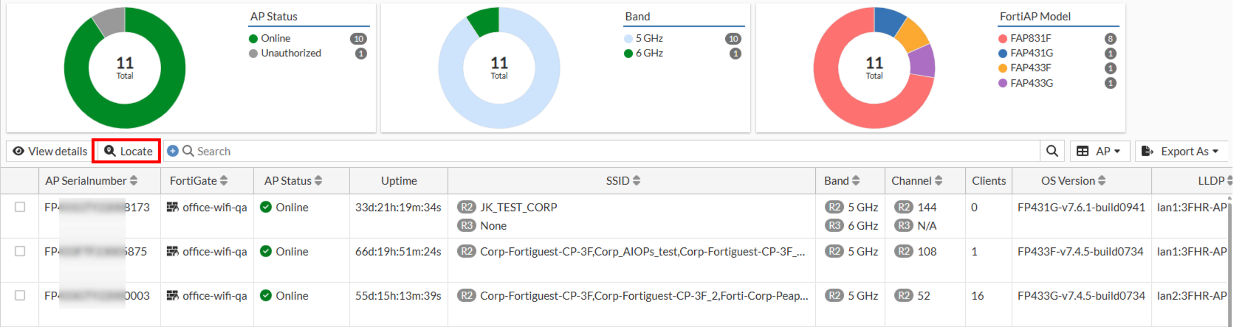
Note: The **Diagnostics and Tools** window is available in both **Unlock Map** and **Lock Map** modes.

Locating Wireless Devices on the Map

This release introduces an enhanced **Locate** feature across the wireless management screens, making it easier to quickly pinpoint the physical location of both Access Points (APs) and wireless clients on your network maps.

Locating Access Points (APs)

The capability to find the physical location of an AP is now accessible from within the **Wireless** > **Access Points** window.



AP Status	
Online	10
Unauthorized	1

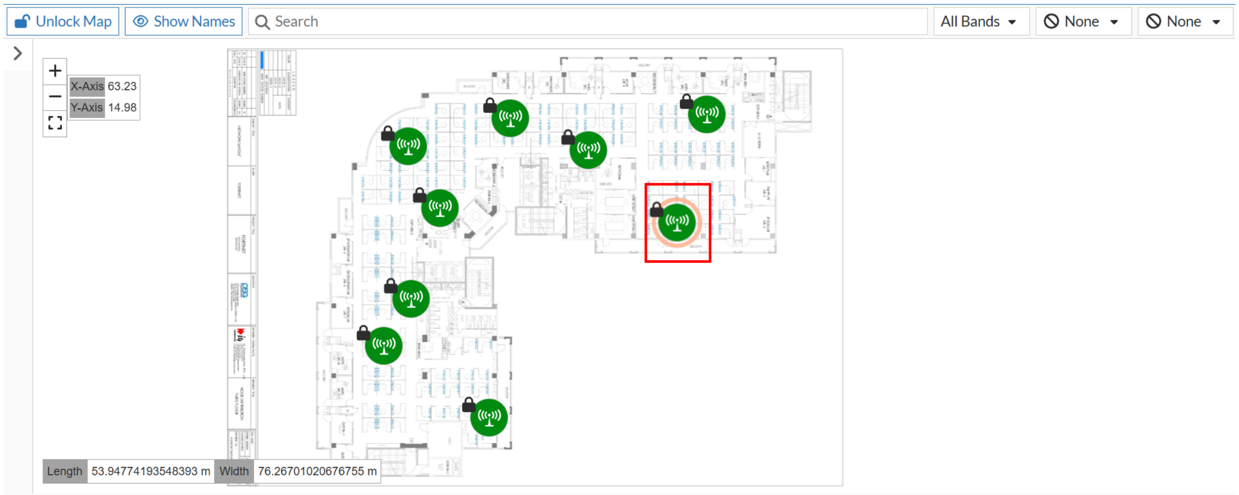
Band	
5 GHz	10
6 GHz	1

FortiAP Model	
FAP831F	8
FAP431G	1
FAP433F	1
FAP433G	1

	AP Serialnumber	FortiGate	AP Status	Uptime	SSID	Band	Channel	Clients	OS Version	LLDP
☐	FP[redacted]8173	office-wifi-qa	Online	33d:21h:19m:34s	R2 JK_TEST_CORP R3 None	R2 5 GHz R3 6 GHz	R2 144 R3 N/A	0	FP431G-v7.6.1-build0941	lan1:3FHR-AP
☐	FP[redacted]5875	office-wifi-qa	Online	66d:19h:51m:24s	R2 Corp-Fortiguest-CP-3F,Corp_AIOPs_test,Corp-Fortiguest-CP-3F_...	R2 5 GHz	R2 108	1	FP433F-v7.4.5-build0734	lan1:3FHR-AP
☐	FP[redacted]0003	office-wifi-qa	Online	55d:15h:13m:39s	R2 Corp-Fortiguest-CP-3F,Corp-Fortiguest-CP-3F_2,Forti-Corp-Peap...	R2 5 GHz	R2 52	16	FP433G-v7.4.5-build0734	lan2:3FHR-AP

The device table now includes a **Locate** option. Select an AP and click **Locate**.

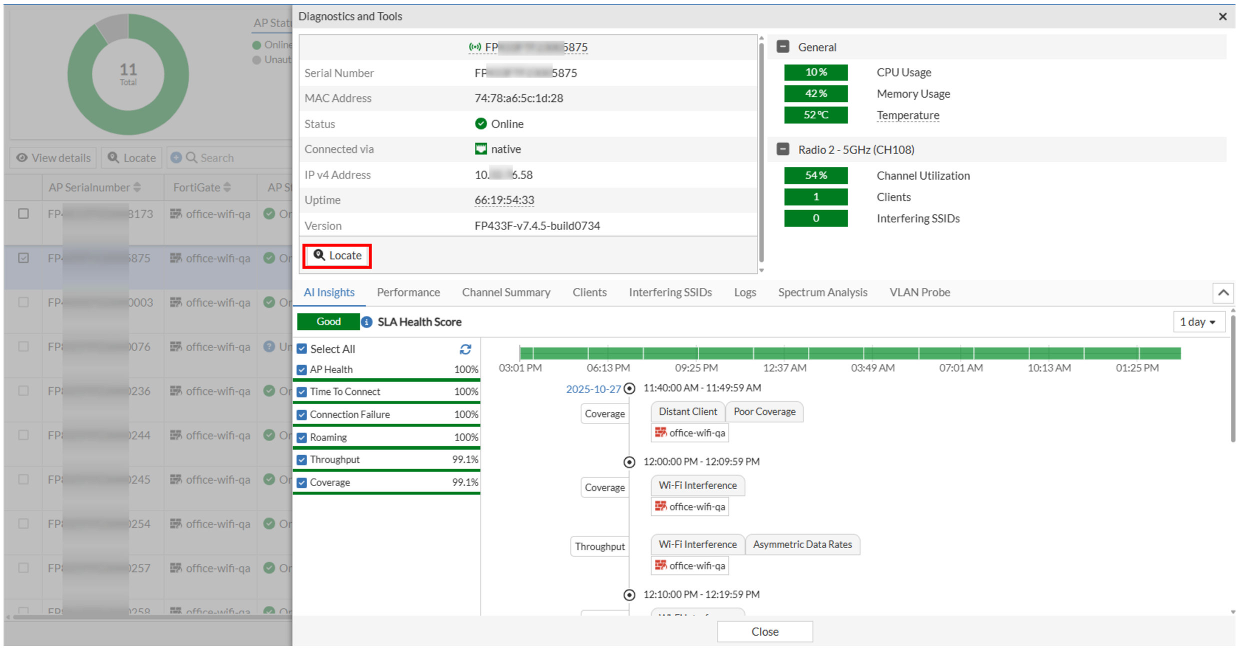
The system opens the **Wi-Fi Maps** window to highlight the placement of the selected AP on its floor plan.



X-Axis 63.23
Y-Axis 14.98

Length 53.94774193548393 m
Width 76.26701020676755 m

The **Diagnostics and Tools** pane has been enhanced with a dedicated **Locate** button. Clicking this button displays the map location of the currently selected AP within the **Wi-Fi Maps** window.



Diagnostics and Tools

FP[redacted]5875

Serial Number	FP[redacted]5875
MAC Address	74:78:a6:5c:1d:28
Status	Online
Connected via	native
IP v4 Address	10.[redacted]6.58
Uptime	66:19:54:33
Version	FP433F-v7.4.5-build0734

Locate

General

10 %	CPU Usage
42 %	Memory Usage
52 °C	Temperature

Radio 2 - 5GHz (CH108)

54 %	Channel Utilization
1	Clients
0	Interfering SSIDs

Good SLA Health Score

1 day

☑ Select All

☑ AP Health	100%
☑ Time To Connect	100%
☑ Connection Failure	100%
☑ Roaming	100%
☑ Throughput	99.1%
☑ Coverage	99.1%

2025-10-27 11:40:00 AM - 11:49:59 AM
Coverage: Distant Client, Poor Coverage — office-wifi-qa

12:00:00 PM - 12:09:59 PM
Coverage: Wi-Fi Interference — office-wifi-qa
Throughput: Wi-Fi Interference, Asymmetric Data Rates — office-wifi-qa

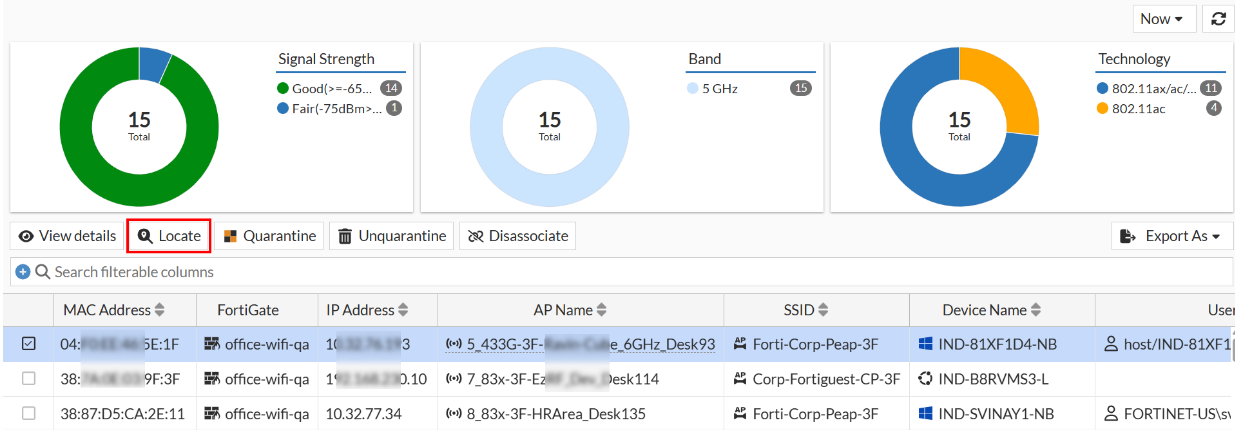
12:10:00 PM - 12:19:59 PM

Close

Locating Wireless Clients

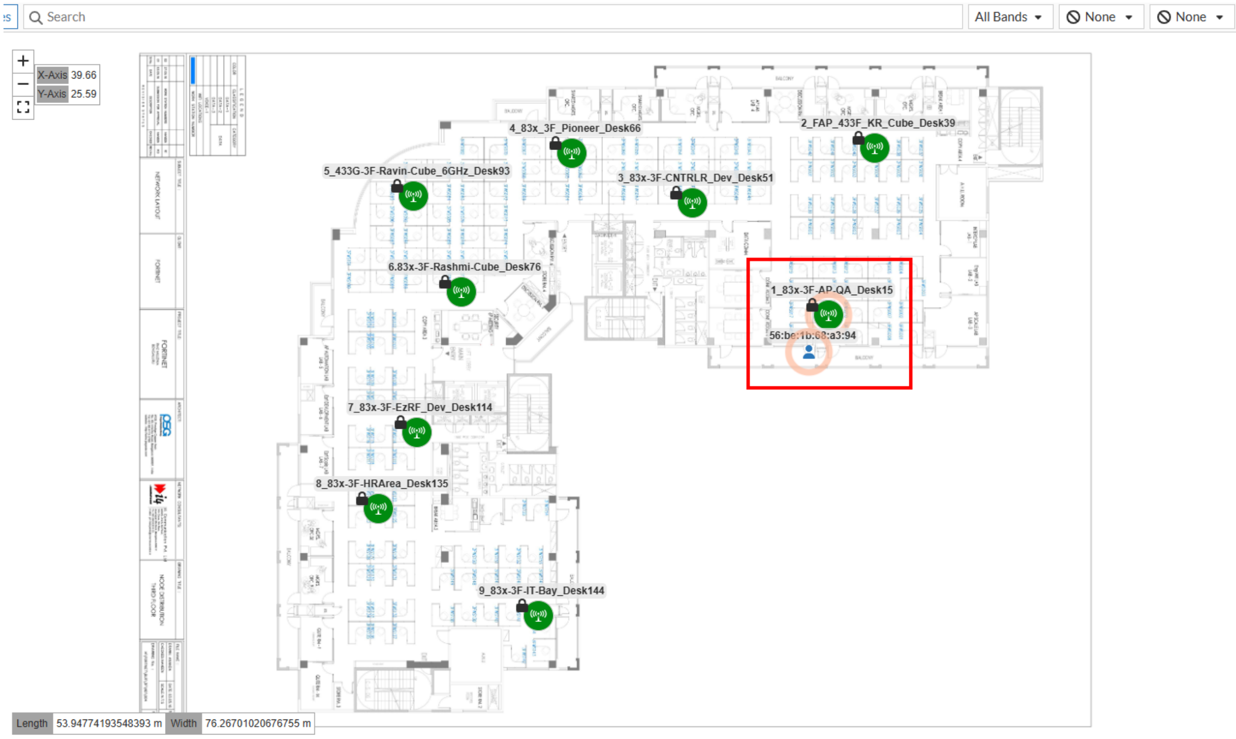
The **Wireless** > **Wireless Clients** window has also been enhanced to include this location capability.

The device table now features a **Locate** option. Select any wireless client and click **Locate**.

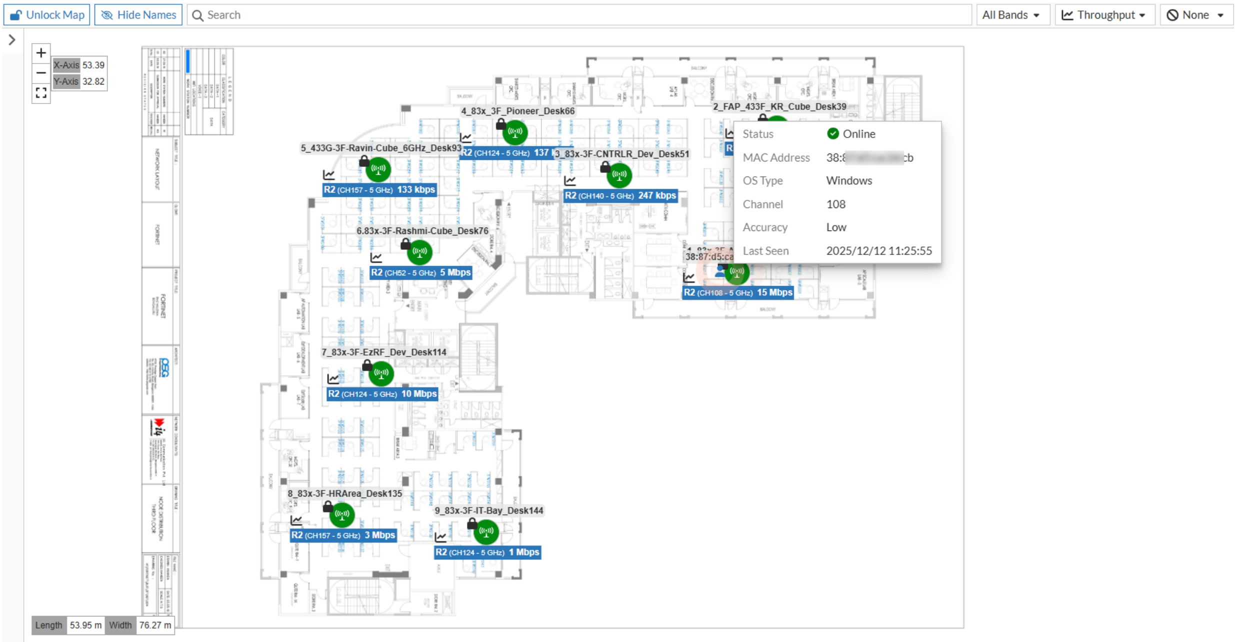


	MAC Address	FortiGate	IP Address	AP Name	SSID	Device Name	User
☑	04:[redacted]5E:1F	office-wifi-qa	10[redacted]3	5_433G-3F-[redacted]e_6GHz_Desk93	Forti-Corp-Peap-3F	IND-81XF1D4-NB	host/IND-81XF1
☐	38:[redacted]9F:3F	office-wifi-qa	19[redacted]0.10	7_83x-3F-Ez[redacted]esk114	Corp-Fortiguest-CP-3F	IND-B8RVMS3-L	
☐	38:87:D5:CA:2E:11	office-wifi-qa	10.32.77.34	8_83x-3F-HRArea_Desk135	Forti-Corp-Peap-3F	IND-SVINAY1-NB	FORTINET-US\s

The system opens the **Wi-Fi Maps** window and highlights the client's physical placement on the floor plan. The AP connected to the wireless client is also highlighted.


Search
All Bands
None
None
X-Axis 39.66
Y-Axis 25.59
4_83x_3F_Pioneer_Desk66
2_FAP_433F_KR_Cube_Desk39
5_433G-3F-Ravin-Cube_6GHz_Desk93
3_83x-3F-CNTRLR_Dev_Desk51
6.83x-3F-Rashmi-Cube_Desk76
1_83x-3F-AP-QA_Desk15
56:be:1b:68:a3:94
7_83x-3F-EzRF_Dev_Desk114
8_83x-3F-HRArea_Desk135
9_83x-3F-IT-Bay_Desk144
Length 53.94774193548393 m
Width 76.26701020676755 m

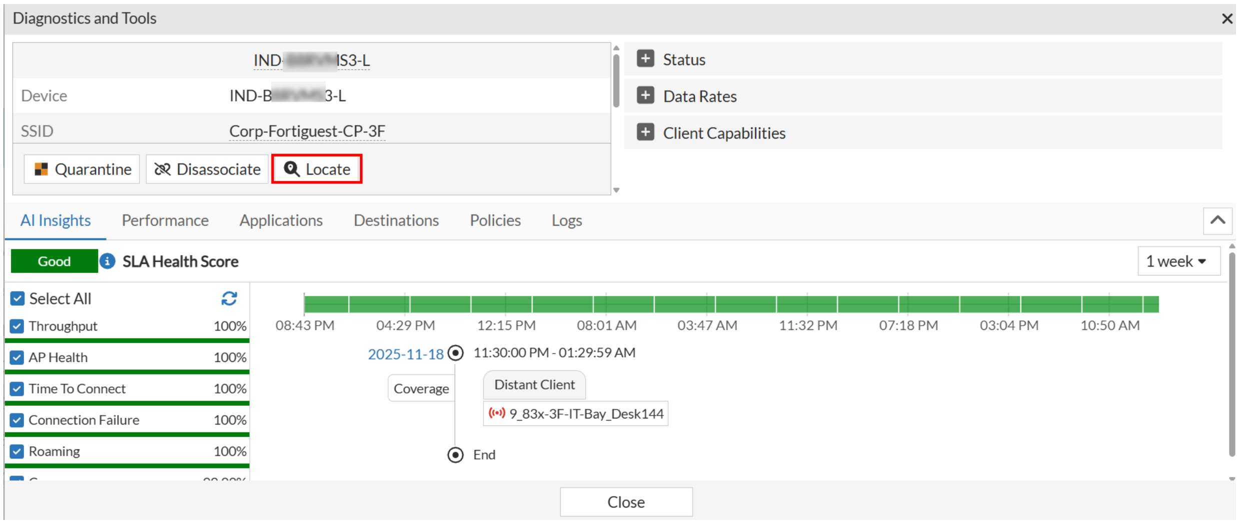
Clicking on the highlighted client will display its detailed information.


Unlock Map
Hide Names
Search
All Bands
Throughput
None
X-Axis 53.39
Y-Axis 32.82
4_83x_3F_Pioneer_Desk66
5_433G-3F-Ravin-Cube_6GHz_Desk93
R2 (CH157 - 5 GHz) 133 kbps
R2 (CH124 - 5 GHz) 137
3_83x-3F-CNTRLR_Dev_Desk51
R2 (CH140 - 5 GHz) 247 kbps
2_FAP_433F_KR_Cube_Desk39
6.83x-3F-Rashmi-Cube_Desk76
R2 (CH52 - 5 GHz) 5 Mbps
38:87:d5:ca
R2 (CH108 - 5 GHz) 15 Mbps
7_83x-3F-EzRF_Dev_Desk114
R2 (CH124 - 5 GHz) 10 Mbps
8_83x-3F-HRArea_Desk135
R2 (CH157 - 5 GHz) 3 Mbps
9_83x-3F-IT-Bay_Desk144
R2 (CH124 - 5 GHz) 1 Mbps
Length 53.95 m
Width 76.27 m

Status	Online
MAC Address	38:[redacted]cb
OS Type	Windows
Channel	108
Accuracy	Low
Last Seen	2025/12/12 11:25:55

Right click on the client to display **Diagnotics and Tools** option for client.

Navigate to **Wireless** > **Wireless Clients** and select an individual client. Click **View Details**. This window displays the **Locate** button which can also be used to locate a client.



IND[redacted]IS3-L

Device	IND-B[redacted]3-L
SSID	Corp-Fortiguest-CP-3F

☑ Select All

☑ Throughput	100%
☑ AP Health	100%
☑ Time To Connect	100%
☑ Connection Failure	100%
☑ Roaming	100%

2025-11-18 11:30:00 PM - 01:29:59 AM

Clicking it shows the map location of the selected wireless client within the **Wi-Fi Maps** window.

FortiExtender Monitoring and Diagnostics

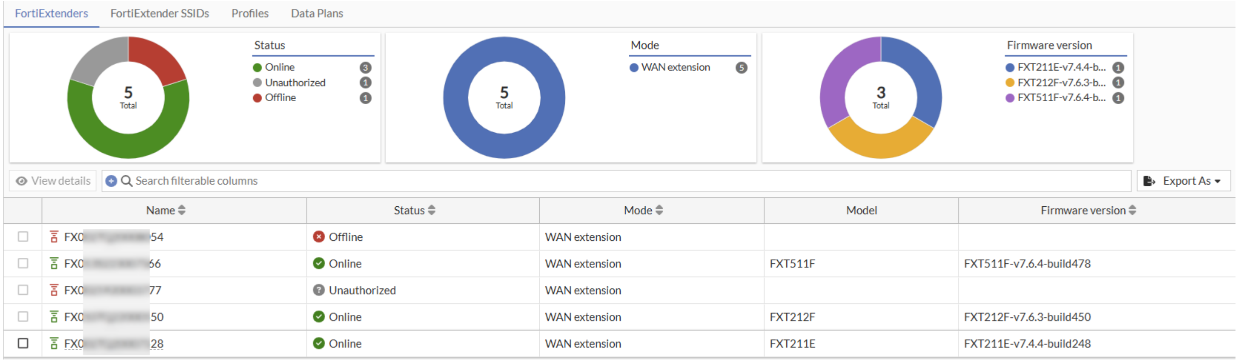
This release introduces a new **FortiExtenders** window that provides a comprehensive view for monitoring all FortiExtender devices across your network, including high-level summaries and in-depth diagnostics.

The **FortiExtender** window is divided into the following tabs:

- FortiExtenders
- FortiExtender SSIDs
- Profiles
- Data Plans

FortiExtenders

The main **FortiExtenders** tab displays both visual summaries in the form of donut charts and a detailed device table.



	Name	Status	Mode	Model	Firmware version
☐	FX0[redacted]54	Offline	WAN extension		
☐	FX0[redacted]66	Online	WAN extension	FXT511F	FXT511F-v7.6.4-build478
☐	FX0[redacted]77	Unauthorized	WAN extension		
☐	FX0[redacted]50	Online	WAN extension	FXT212F	FXT212F-v7.6.3-build450
☐	FX0[redacted]28	Online	WAN extension	FXT211E	FXT211E-v7.4.4-build248

Following charts are available:

- Status: Shows the total number of FortiExtenders that are Online versus Offline.
- Mode: Displays the number of devices based on their mode of operation: WAN extension mode or LAN extension mode.
- Firmware Version: Displays a count of devices grouped by their current firmware version.

The device table lists the following information for all FortiExtenders:

Name	Name of the FortiExtender
Status	Fortiextender status (online or offline)
Mode	Mode of operation (WAN extension or LAN extension)
Model	FortiExtender model
Firmware Version	FortiExtender firmware version
Data Usage	Current data usage
Details	FortiExtender details

ESN IMEI	FortiExtender electronic serial number (ESN) and international mobile equipment identity (IMEI)
FortiGate IP Address	IP address of FortiGate device
FortiGate Serial Number	Serial number of FortiGate device
ICCID	FortiExtender integrated circuit card identity (ICCID) number
IMSI	FortiExtender international mobile subscriber identity (IMSI) number
IP Address	FortiExtender IP address
Modem 1 interface	Name of the Modem 1 Interface
Modem 2 Interface	Name of the Modem 2 Interface
Network	FortiExtender carrier name
Phone Number	FortiExtender phone number
Profile	Profile name of the FortiExtender
RSRP	The Reference Signal Received Power
RSRQ	The Reference Signal Received Quality
RSSI	The Received Signal Strength Indicator
Serial Number	Serial number of the FortiExtender
SINR	The Signal-to-Interference-plus-Noise Ratio
Temperature	Temperature information of FortiExtender
VDOM	Virtual domain

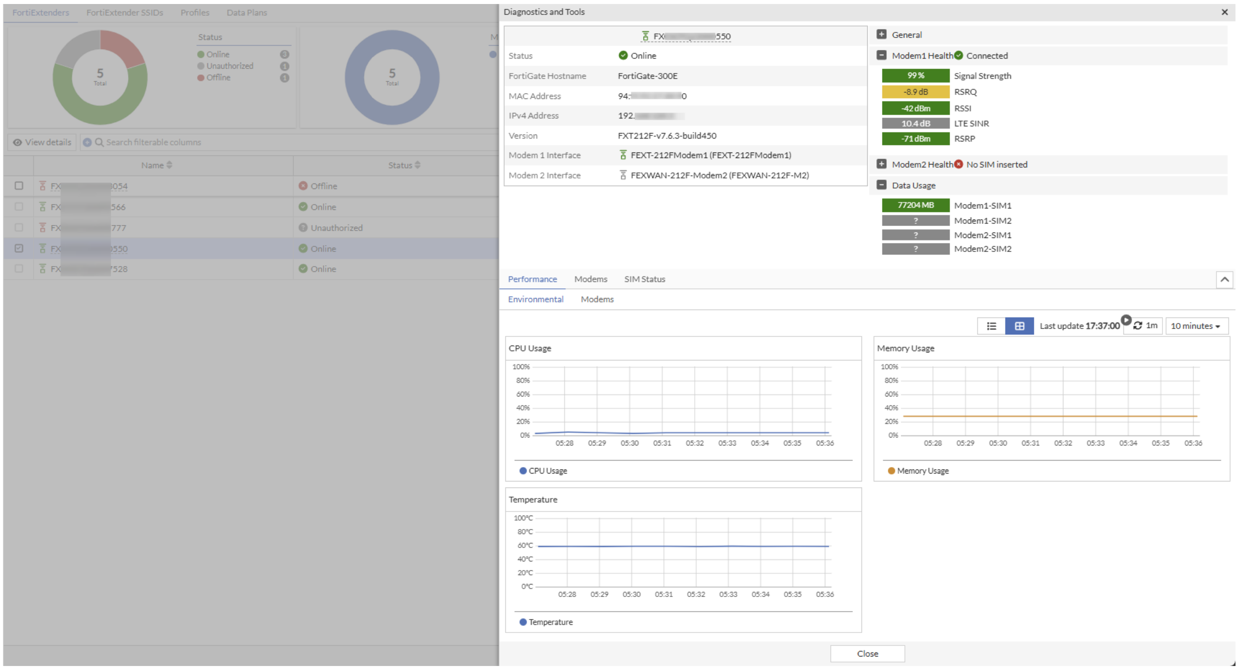
The **Export As** option enables you to export the table data (filtered or all data) in formats like CSV, JSON, Plaintext, or PDF.

Note: You can customize the exported data by selecting up to 8 columns to include in the file.

To access detailed statistics and troubleshoot a device, select a FortiExtender from the table and click **View Details.** This opens the **Diagnostics and Tools** pane, which contains the following tabs:

- Performance
- Modems
- SIM Status

Performance



FX[redacted]550

Status	Online
FortiGate Hostname	FortiGate-300E
MAC Address	94:[redacted]0
IPv4 Address	192.[redacted]
Version	FXT212F-v7.6.3-build450
Modem 1 Interface	FEXT-212FModem1 (FEXT-212FModem1)
Modem 2 Interface	FEXWAN-212F-Modem2 (FEXWAN-212F-M2)

Modem1 Health Connected

99 %	Signal Strength
-8.9 dB	RSRQ
-42 dBm	RSSI
10.4 dB	LTE SINR
-71 dBm	RSRP

Modem2 Health No SIM inserted

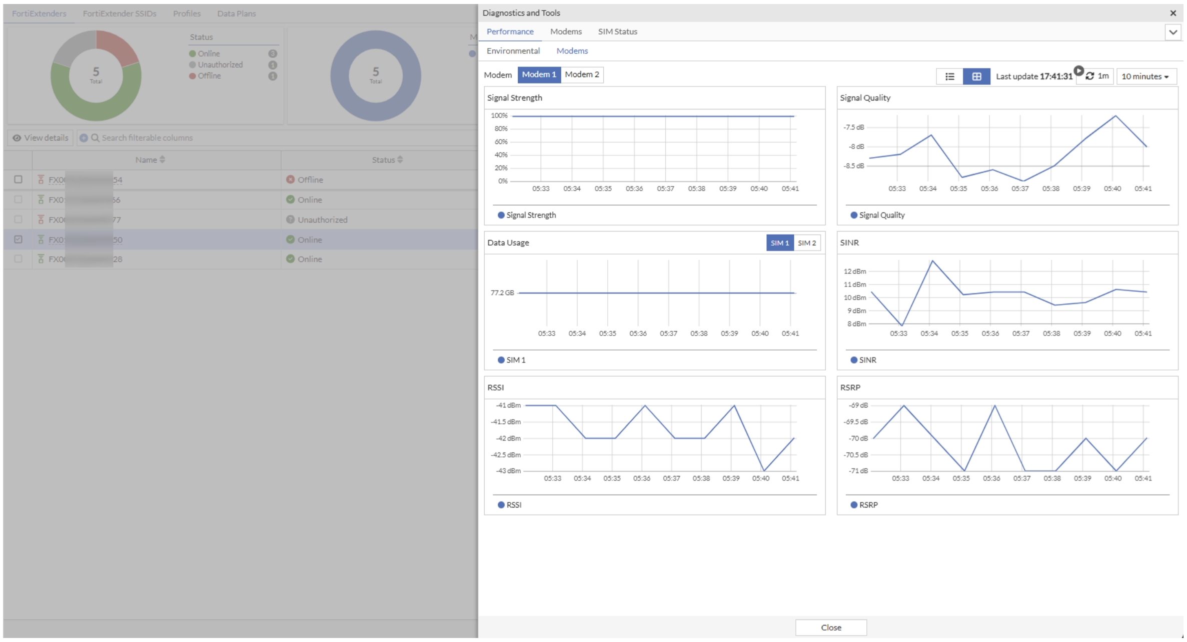
Data Usage

77204 MB	Modem1-SIM1
?	Modem1-SIM2
?	Modem2-SIM1
?	Modem2-SIM2

Last update 17:37:00 1m 10 minutes

This tab displays charts tracking the FortiExtender's health and usage:

- **Environmental**: The Environmental sub-tab provides critical charts detailing the FortiExtender's environmental and resource health over the specified time period. The following charts are available:
    - CPU Usage
    - Memory Usage
    - Temperature
- **Modems**: The Modems sub-tab provides critical performance metrics for both Modem 1 and Modem 2 over a specified time period.

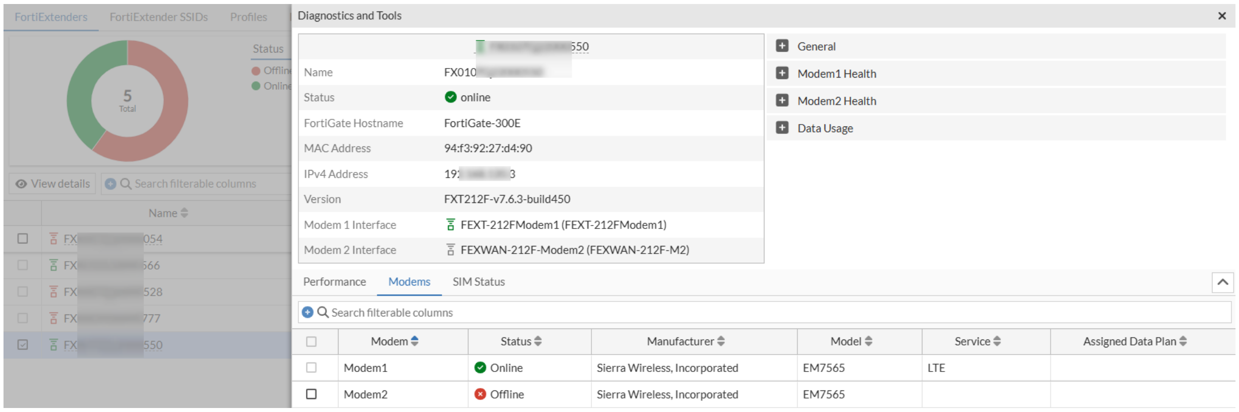


Last update 17:41:31 1m 10 minutes

These details are presented through individual charts for each of the following

- Signal Strength
- Signal Quality
- Data Usage
- SINR (Signal-to-Interference-plus-Noise Ratio)
- RSSI (Received Signal Strength Indicator)
- RSRP (Reference Signal Received Power)

Modems



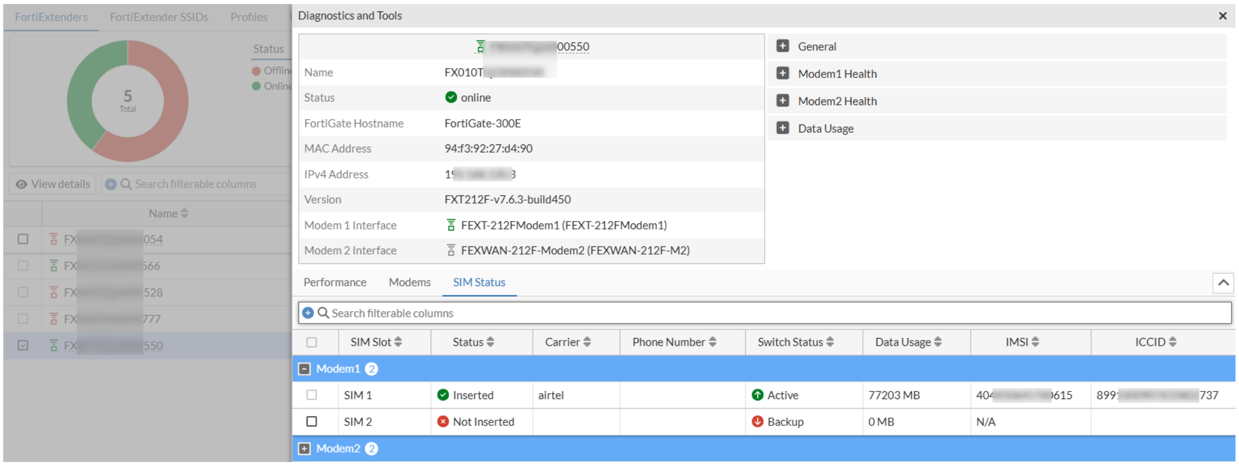
[redacted]550

Name FX010[redacted]
Status online
FortiGate Hostname FortiGate-300E
MAC Address 94:f3:92:27:d4:90
IPv4 Address 19[redacted]3
Version FXT212F-v7.6.3-build450
Modem 1 Interface FEXT-212FModem1 (FEXT-212FModem1)
Modem 2 Interface FEXWAN-212F-Modem2 (FEXWAN-212F-M2)

☐	Modem	Status	Manufacturer	Model	Service	Assigned Data Plan
☐	Modem1	Online	Sierra Wireless, Incorporated	EM7565	LTE	
☐	Modem2	Offline	Sierra Wireless, Incorporated	EM7565		

This tab provides key hardware and configuration details for the FortiExtender's modems. Details such as Status, Manufacturer, Assigned Data Plan, Service, and Model of the modems are displayed.

SIM Status



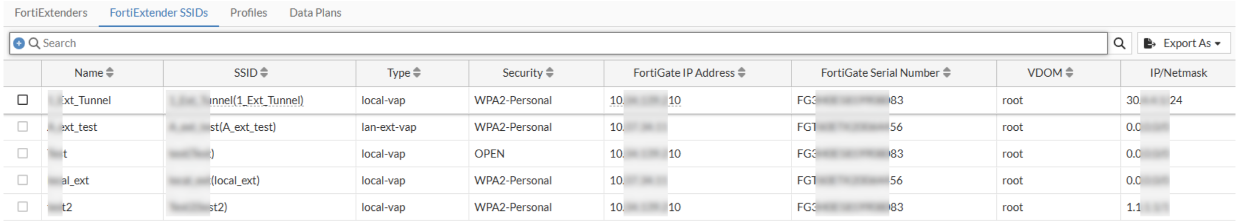
[redacted]00550

Name FX010T[redacted]
Status online
FortiGate Hostname FortiGate-300E
MAC Address 94:f3:92:27:d4:90
IPv4 Address 19[redacted]3
Version FXT212F-v7.6.3-build450
Modem 1 Interface FEXT-212FModem1 (FEXT-212FModem1)
Modem 2 Interface FEXWAN-212F-Modem2 (FEXWAN-212F-M2)

☐	SIM Slot	Status	Carrier	Phone Number	Switch Status	Data Usage	IMSI	ICCID
Modem1 ②								
☐	SIM 1	Inserted	airtel		Active	77203 MB	404[redacted]615	899[redacted]737
☐	SIM 2	Not Inserted			Backup	0 MB	N/A	
Modem2 ②								

The **SIM Status** tab displays details for the cellular Subscriber Identity Modules (SIMs) in the modems. The information displayed for each SIM includes Status, Carrier, Phone Number, Switch Status, Data Usage, IMSI, and ICCID related to both SIM 1 and SIM 2 of the Modems available.

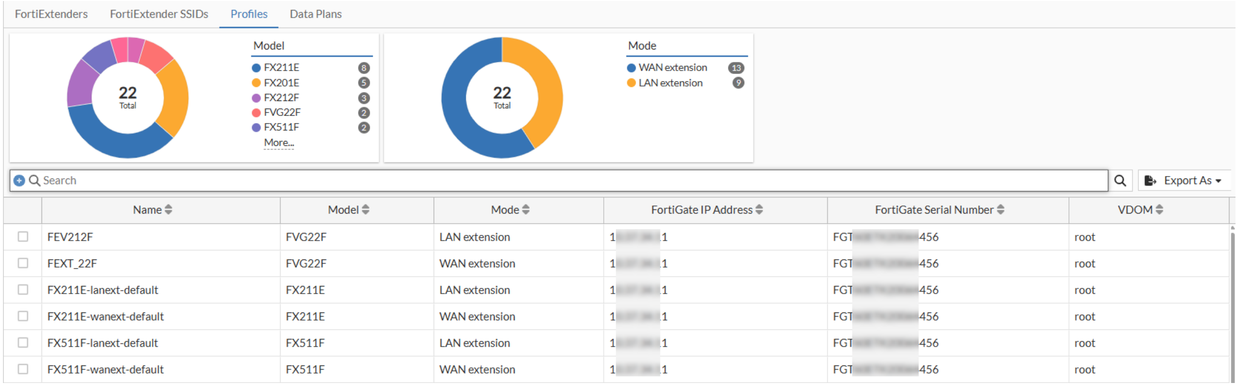
FortiExtender SSIDs



	Name	SSID	Type	Security	FortiGate IP Address	FortiGate Serial Number	VDOM	IP/Netmask
☐	[redacted]xt_Tunnel	[redacted]nnel(1_Ext_Tunnel)	local-vap	WPA2-Personal	10.[redacted]10	FG3[redacted]83	root	30.[redacted]24
☐	[redacted]ext_test	[redacted]st(A_ext_test)	lan-ext-vap	WPA2-Personal	10.[redacted]	FGT[redacted]56	root	0.0[redacted]
☐	[redacted]t	[redacted])	local-vap	OPEN	10.[redacted]10	FG3[redacted]83	root	0.0[redacted]
☐	[redacted]al_ext	[redacted](local_ext)	local-vap	WPA2-Personal	10.[redacted]	FGT[redacted]56	root	0.0[redacted]
☐	[redacted]t2	[redacted]st2)	local-vap	WPA2-Personal	10.[redacted]10	FG3[redacted]83	root	1.1[redacted]

This tab lists SSID configuration details, including Name, SSID, Type, Security, FortiGate IP Address, FortiGate Serial Number, VDOM, and IP/Netmask.

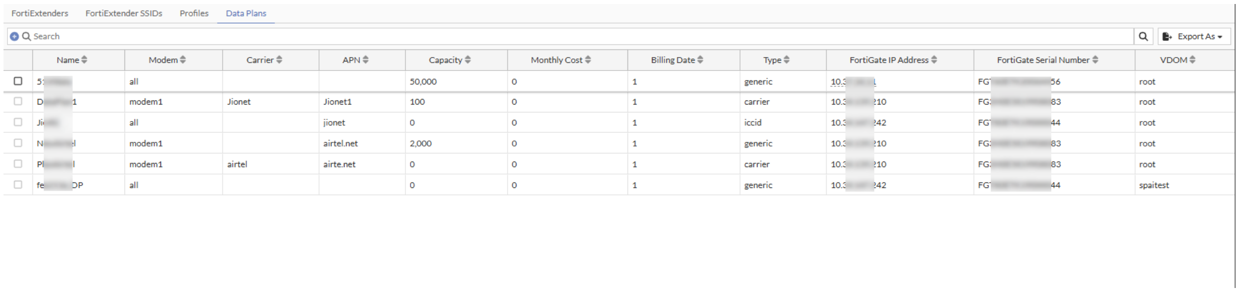
Profiles



	Name	Model	Mode	FortiGate IP Address	FortiGate Serial Number	VDOM
☐	FEV212F	FVG22F	LAN extension	1[redacted]1	FGT[redacted]456	root
☐	FEXT_22F	FVG22F	WAN extension	1[redacted]1	FGT[redacted]456	root
☐	FX211E-lanext-default	FX211E	LAN extension	1[redacted]1	FGT[redacted]456	root
☐	FX211E-wanext-default	FX211E	WAN extension	1[redacted]1	FGT[redacted]456	root
☐	FX511F-lanext-default	FX511F	LAN extension	1[redacted]1	FGT[redacted]456	root
☐	FX511F-wanext-default	FX511F	WAN extension	1[redacted]1	FGT[redacted]456	root

This tab displays information about configuration profiles, such as Name, Model, Mode, FortiGate IP Address, FortiGate Serial Number, and VDOM.

Data Plans



	Name	Modem	Carrier	APN	Capacity	Monthly Cost	Billing Date	Type	FortiGate IP Address	FortiGate Serial Number	VDOM
☐	5[redacted]	all			50,000	0	1	generic	10.3[redacted]1	FG[redacted]56	root
☐	D[redacted]1	modem1	Jionet	Jionet1	100	0	1	carrier	10.3[redacted]210	FG[redacted]83	root
☐	Ji[redacted]	all		jionet	0	0	1	iccid	10.3[redacted]242	FG[redacted]44	root
☐	N[redacted]l	modem1		airtel.net	2,000	0	1	generic	10.3[redacted]210	FG[redacted]83	root
☐	Pl[redacted]l	modem1	airtel	airte.net	0	0	1	carrier	10.3[redacted]210	FG[redacted]83	root
☐	fe[redacted]DP	all			0	0	1	generic	10.3[redacted]242	FG[redacted]44	spaitest

This tab shows all configured cellular data plans, including Name, Modem, Carrier, APN, Capacity, Monthly Cost, Billing Date, Type, FortiGate IP Address, FortiGate Serial Number, and VDOM.

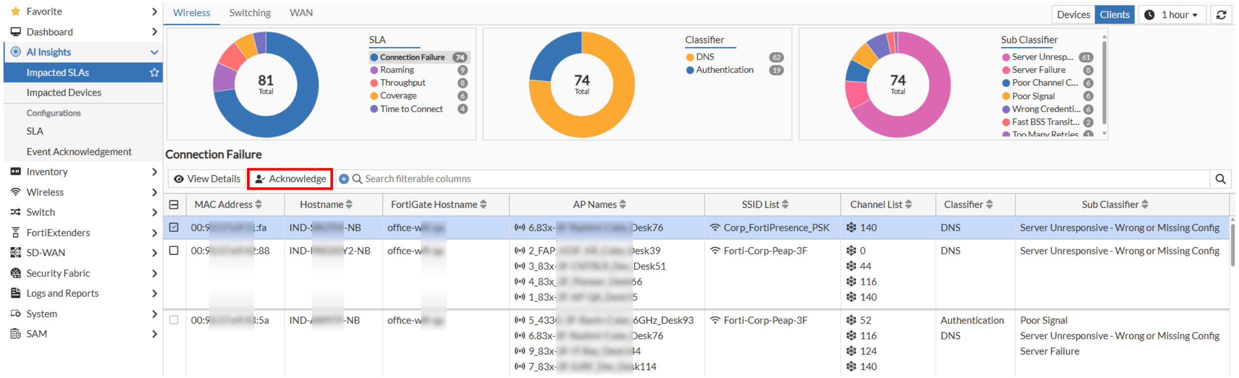
Advanced Alert Acknowledgement

This release introduces a robust way to manage false positives and SLA violations, giving you more control over your network monitoring and reporting.

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

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

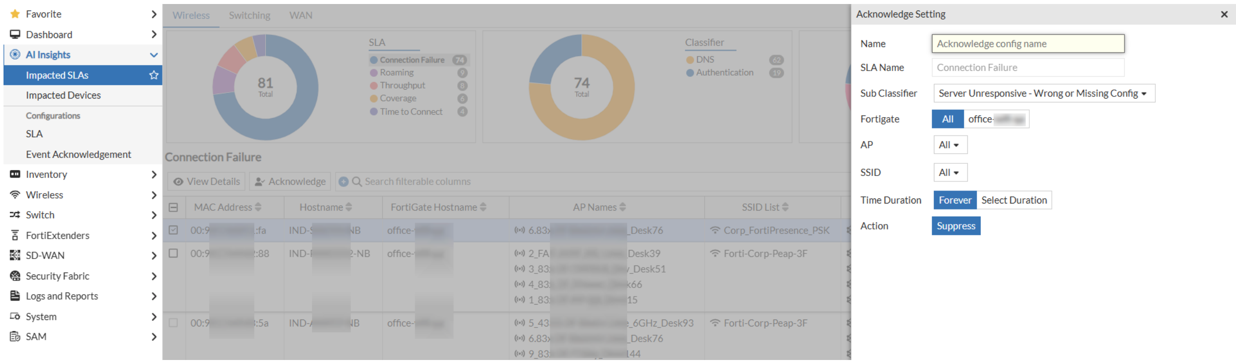
You can set up new acknowledgements directly from the **AI Insights** > **Impacted SLA** window.



Connection Failure

☐	MAC Address	Hostname	FortiGate Hostname	AP Names	SSID List	Channel List	Classifier	Sub Classifier
☑	00:9[redacted]:fa	IND-[redacted]-NB	office-w[redacted]	6.83x-[redacted]Desk76	Corp_FortiPresence_PSK	140	DNS	Server Unresponsive - Wrong or Missing Config
☐	00:9[redacted]:88	IND-[redacted]Y2-NB	office-w[redacted]	2_FAP[redacted]Desk39 3_83x-[redacted]Desk51 4_83x_[redacted]66 1_83x-[redacted]5	Forti-Corp-Peap-3F	0 44 116 140	DNS	Server Unresponsive - Wrong or Missing Config
☐	00:9[redacted]:5a	IND-[redacted]-NB	office-w[redacted]	5_433[redacted]6GHz_Desk93 6.83x-[redacted]Desk76 9_83x-[redacted]44 7_83x-[redacted]k114	Forti-Corp-Peap-3F	52 116 124 140	Authentication DNS	Poor Signal Server Unresponsive - Wrong or Missing Config Server Failure

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



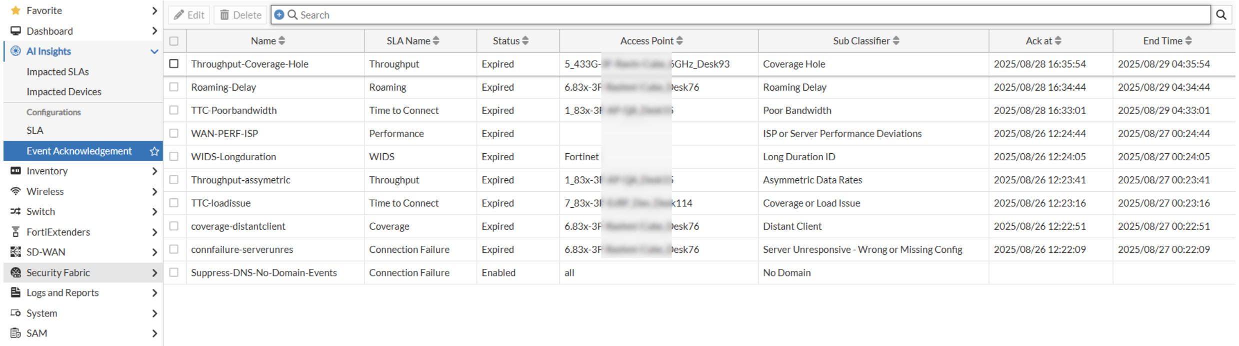
Name: Acknowledge config name
SLA Name: Connection Failure
Sub Classifier: Server Unresponsive - Wrong or Missing Config
Fortigate: All | office-[redacted]
AP: All
SSID: All
Time Duration: Forever | Select Duration
Action: Suppress

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

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

Configure all the other necessary settings.

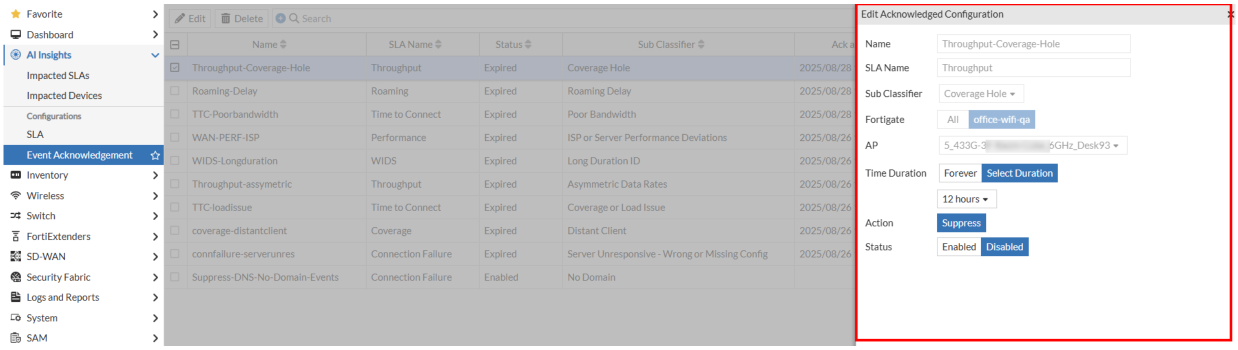
All the configured acknowledgements are available on the new **Event Acknowledgement** window. Navigate to **AI Insights** > **Event Acknowledgement**.



☐	Name	SLA Name	Status	Access Point	Sub Classifier	Ack at	End Time
☐	Throughput-Coverage-Hole	Throughput	Expired	5_433G-[redacted]GHz_Desk93	Coverage Hole	2025/08/28 16:35:54	2025/08/29 04:35:54
☐	Roaming-Delay	Roaming	Expired	6.83x-3F[redacted]esk76	Roaming Delay	2025/08/28 16:34:44	2025/08/29 04:34:44
☐	TTC-Poorbandwidth	Time to Connect	Expired	1_83x-3F[redacted]	Poor Bandwidth	2025/08/28 16:33:01	2025/08/29 04:33:01
☐	WAN-PERF-ISP	Performance	Expired		ISP or Server Performance Deviations	2025/08/26 12:24:44	2025/08/27 00:24:44
☐	WIDS-Longduration	WIDS	Expired	Fortinet	Long Duration ID	2025/08/26 12:24:05	2025/08/27 00:24:05
☐	Throughput-assymetric	Throughput	Expired	1_83x-3F[redacted]	Asymmetric Data Rates	2025/08/26 12:23:41	2025/08/27 00:23:41
☐	TTC-loadissue	Time to Connect	Expired	7_83x-3F[redacted]k114	Coverage or Load Issue	2025/08/26 12:23:16	2025/08/27 00:23:16
☐	coverage-distantclient	Coverage	Expired	6.83x-3F[redacted]esk76	Distant Client	2025/08/26 12:22:51	2025/08/27 00:22:51
☐	connfailure-serverunres	Connection Failure	Expired	6.83x-3F[redacted]esk76	Server Unresponsive - Wrong or Missing Config	2025/08/26 12:22:09	2025/08/27 00:22:09
☐	Suppress-DNS-No-Domain-Events	Connection Failure	Enabled	all	No Domain		

You can edit an acknowledgement to

- **Enable**/**Disable** a setting to temporarily pause or resume an acknowledgement.
- Change the **Time Duration** of an existing rule.



Edit Acknowledged Configuration

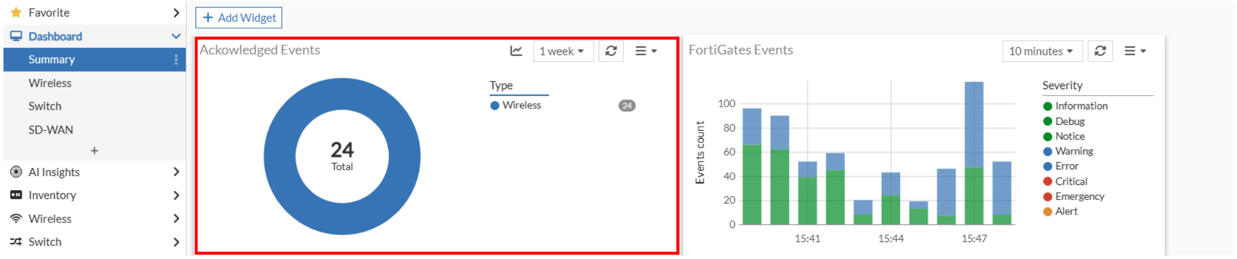
Name: Throughput-Coverage-Hole
SLA Name: Throughput
Sub Classifier: Coverage Hole
Fortigate: All | office-wifi-qa
AP: 5_433G-3[redacted]GHz_Desk93
Time Duration: Forever | Select Duration
12 hours
Action: Suppress
Status: Enabled | Disabled

From the **Event Acknowledgement** window, select an acknowledgement to **Delete** it.

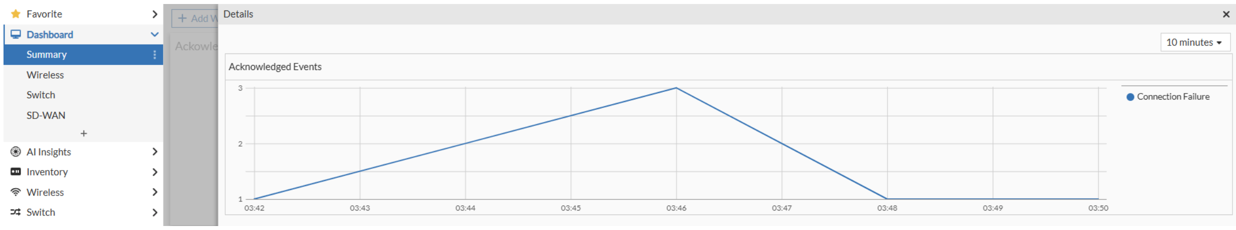
Acknowledged Events Widget

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

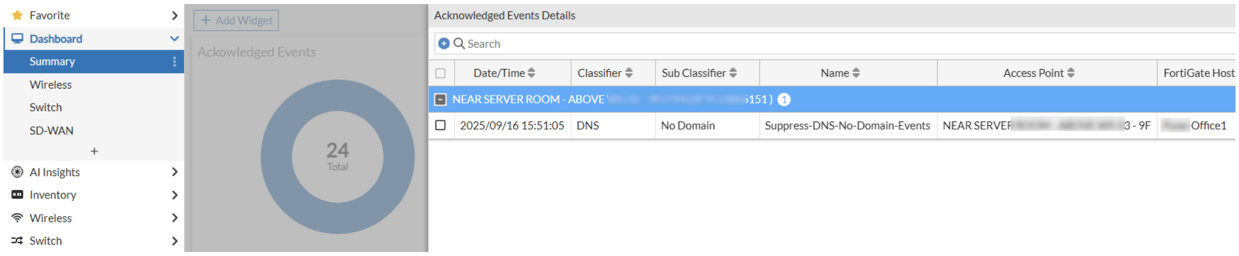
To add the widget, navigate to **Dashboard** > **Summary**. Click **Add Widget**.



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



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

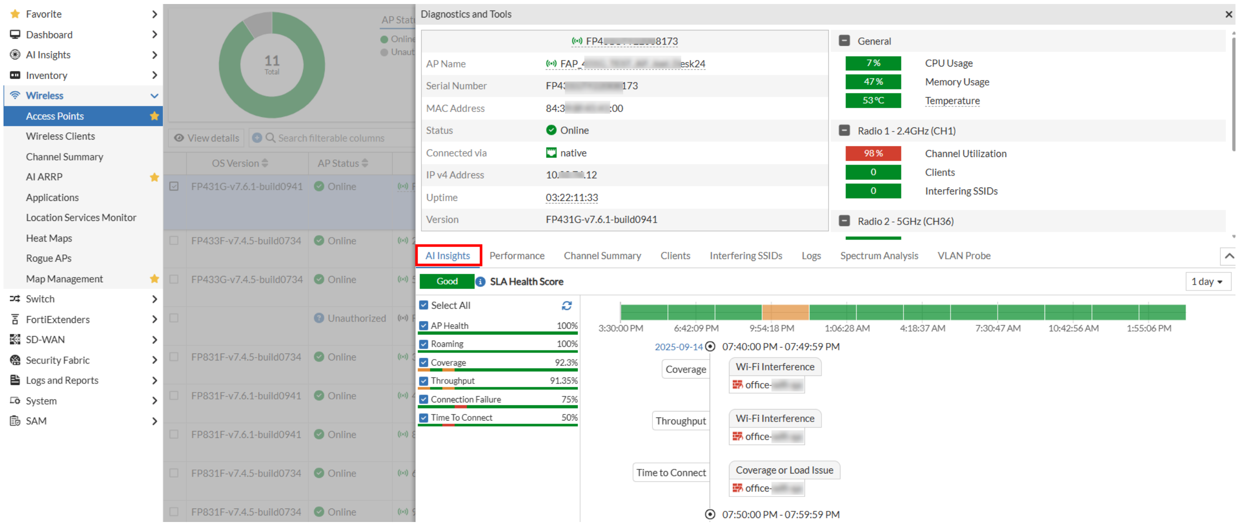


☐	Date/Time	Classifier	Sub Classifier	Name	Access Point	FortiGate Host
☐	NEAR SERVER ROOM - ABOVE [redacted] 151) 1					
☐	2025/09/16 15:51:05	DNS	No Domain	Suppress-DNS-No-Domain-Events	NEAR SERVER [redacted] 3 - 9F	[redacted] Office1

AI Insights for Network Health Monitoring

This release introduces **AI Insights** tab in the **Diagnostics and Tools** window for Access Points, Wireless Clients, and FortiSwitches. This new tab helps to analyze various performance metrics, identify issues, and provide detailed insights into the root cause of network problems, helping administrators maintain high service levels.

Note: In this release, the feature may not work as expected on Safari browser. For the best experience, use Chrome, Firefox, or Microsoft Edge instead.



Diagnostics and Tools

FP4[redacted]8173

AP Name	FAP_[redacted]esk24
Serial Number	FP4[redacted]173
MAC Address	84:3[redacted]:00
Status	Online
Connected via	native
IP v4 Address	10.[redacted].12
Uptime	03:22:11:33
Version	FP431G-v7.6.1-build0941

General

7 %	CPU Usage
47 %	Memory Usage
53 °C	Temperature

Radio 1 - 2.4GHz (CH1)

98 %	Channel Utilization
0	Clients
0	Interfering SSIDs

Radio 2 - 5GHz (CH36)

AP list		
FP431F-v7.6.1-build0941	Online	
FP433F-v7.4.5-build0734	Online	
FP433G-v7.4.5-build0734	Online	
	Unauthorized	
FP831F-v7.4.5-build0734	Online	
FP831F-v7.6.1-build0941	Online	
FP831F-v7.6.1-build0941	Online	
FP831F-v7.4.5-build0734	Online	
FP831F-v7.4.5-build0734	Online	

Good SLA Health Score

☑ Select All

☑ AP Health	100%
☑ Roaming	100%
☑ Coverage	92.3%
☑ Throughput	91.35%
☑ Connection Failure	75%
☑ Time To Connect	50%

2025-09-14 07:40:00 PM - 07:49:59 PM

Coverage — Wi-Fi Interference — office-[redacted]

Throughput — Wi-Fi Interference — office-[redacted]

Time to Connect — Coverage or Load Issue — office-[redacted]

07:50:00 PM - 07:59:59 PM

The **SLA Health Score** provides the overall high-level score.

- **Good** for a score more 70
- **Fair** for a score between 30 and 70
- **Bad** for a score less than 30

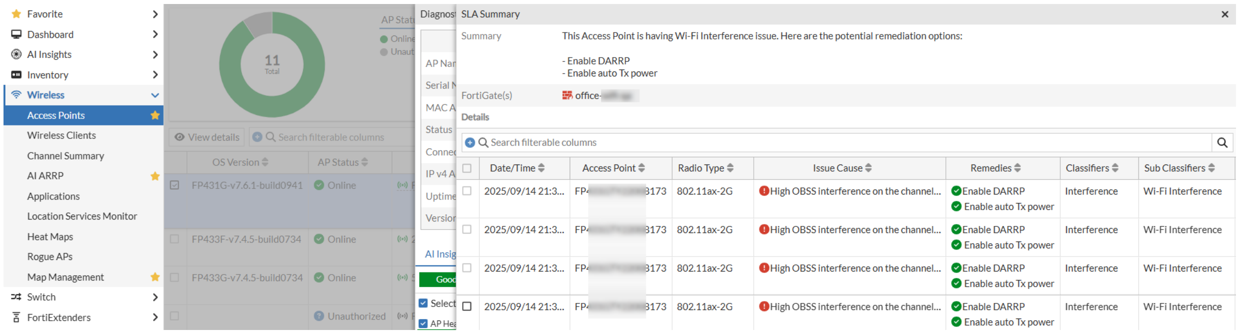
Below the overall score, a list of individual SLAs or metrics is shown with their current health scores. You can select the SLAs that you want to track.

The following metrics are available:

Device	SLA
Access Points and Wireless Clients	• AP Health • Roaming • Coverage • Throughput • Connection Failure • Time To Connect
FortiSwitches	• Switch Network • Switch Throughput

Device	SLA
	• Switch Health and Uptime • Switch Connection Failure

When you click an SLA, the corresponding **SLA Summary** window opens with more details.



Summary: This Access Point is having Wi-Fi Interference issue. Here are the potential remediation options:

- Enable DARRP
- Enable auto Tx power

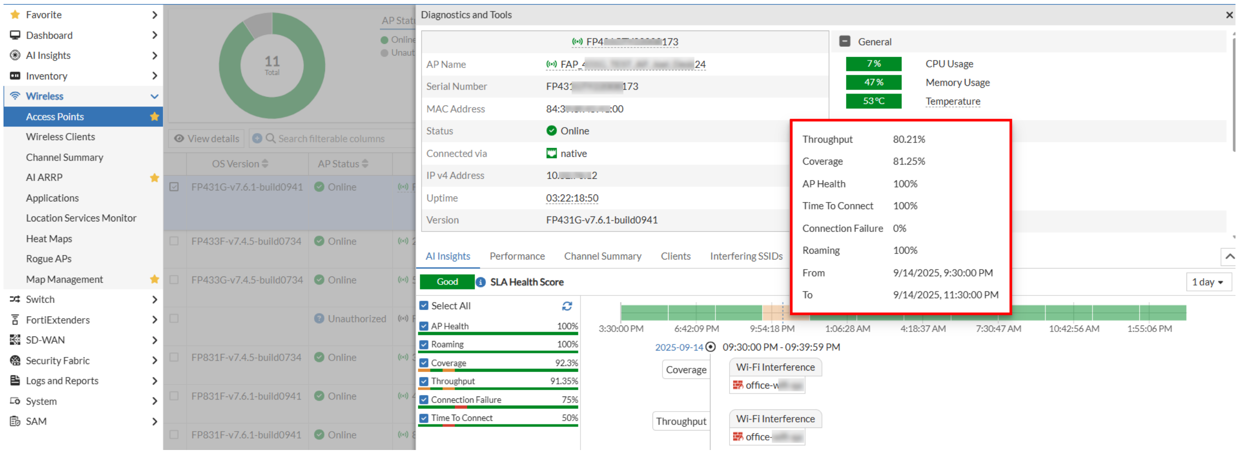
FortiGate(s): office-[redacted]

Details

☐	Date/Time	Access Point	Radio Type	Issue Cause	Remedies	Classifiers	Sub Classifiers
☐	2025/09/14 21:3...	FP4[redacted]3173	802.11ax-2G	High OBSS interference on the channel...	✓ Enable DARRP ✓ Enable auto Tx power	Interference	Wi-Fi Interference
☐	2025/09/14 21:3...	FP4[redacted]3173	802.11ax-2G	High OBSS interference on the channel...	✓ Enable DARRP ✓ Enable auto Tx power	Interference	Wi-Fi Interference
☐	2025/09/14 21:3...	FP4[redacted]3173	802.11ax-2G	High OBSS interference on the channel...	✓ Enable DARRP ✓ Enable auto Tx power	Interference	Wi-Fi Interference
☐	2025/09/14 21:3...	FP4[redacted]3173	802.11ax-2G	High OBSS interference on the channel...	✓ Enable DARRP ✓ Enable auto Tx power	Interference	Wi-Fi Interference

The bar graph shows the performance trend over a selected time period (in this case, 1 day). The graph is divided to equal time segments. Based on the health score of each segment, the segments are colour coded as green (good), orange (fair), and red (bad).

Clicking on a specific time segment (for example, an orange bar) displays more details events that occurred during the time period.



FP4[redacted]173

AP Name	FAP_4[redacted]24
Serial Number	FP431[redacted]173
MAC Address	84:3[redacted]:00
Status	Online
Connected via	native
IP v4 Address	10.[redacted]2
Uptime	03:22:18:50
Version	FP431G-v7.6.1-build0941

7 %	CPU Usage
47 %	Memory Usage
53 °C	Temperature

Throughput	80.21%
Coverage	81.25%
AP Health	100%
Time To Connect	100%
Connection Failure	0%
Roaming	100%
From	9/14/2025, 9:30:00 PM
To	9/14/2025, 11:30:00 PM

Good SLA Health Score

☑ Select All	
☑ AP Health	100%
☑ Roaming	100%
☑ Coverage	92.3%
☑ Throughput	91.35%
☑ Connection Failure	75%
☑ Time To Connect	50%

2025-09-14 09:30:00 PM - 09:39:59 PM

Coverage: Wi-Fi Interference, office-w[redacted]

Throughput: Wi-Fi Interference, office-[redacted]

Enhanced Monitoring for Wireless Clients

This release introduces new ways to monitor and troubleshoot network performance. You can now view and analyze trends for signal strength and data rates, and take immediate action on client devices.

The following windows are updated:

- Diagnostics and Tools
- Wireless Dashboard

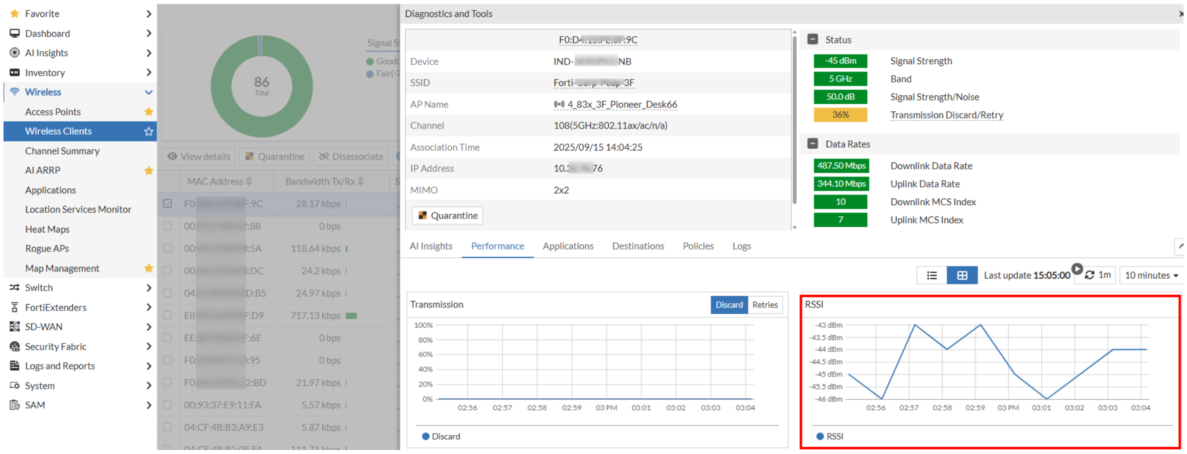
Diagnostics and Tools

The Diagnostics and Tools pane is updated with the following changes:

Performance Tab

The following charts are added to the Performance tab:

- **RSSI Chart**: This chart displays the trend of Received Signal Strength Indicator (RSSI) over a selected time period for a client. RSSI is a measure of the Wi-Fi signal strength your device receives from an Access Point, typically measured in dBm (decibel milliwatts). A value closer to 0 dBm (for example, -30 dBm) indicates a strong signal, while a value closer to -90 dBm indicates a very poor one.



MAC Address	Bandwidth Tx/Rx
F0[redacted]F:9C	28.17 kbps
00[redacted]2:88	0 bps
00[redacted]3:5A	118.64 kbps
00[redacted]3:DC	24.2 kbps
04[redacted]D:B5	24.97 kbps
E8[redacted]F:D9	717.13 kbps
EE[redacted]F:6E	0 bps
F0[redacted]0:95	0 bps
F0[redacted]2:BD	21.97 kbps
00:93:37:E9:11:FA	5.57 kbps
04:CF:4B:B3:A9:E3	5.87 kbps

	F0:D4[redacted]:9C
Device	IND-[redacted]NB
SSID	Forti-[redacted]3F
AP Name	4_83x_3F_Pioneer_Desk66
Channel	108(5GHz:802.11ax/ac/n/a)
Association Time	2025/09/15 14:04:25
IP Address	10.[redacted]76
MIMO	2x2

Status

-45 dBm	Signal Strength
5 GHz	Band
50.0 dB	Signal Strength/Noise
36%	Transmission Discard/Retry

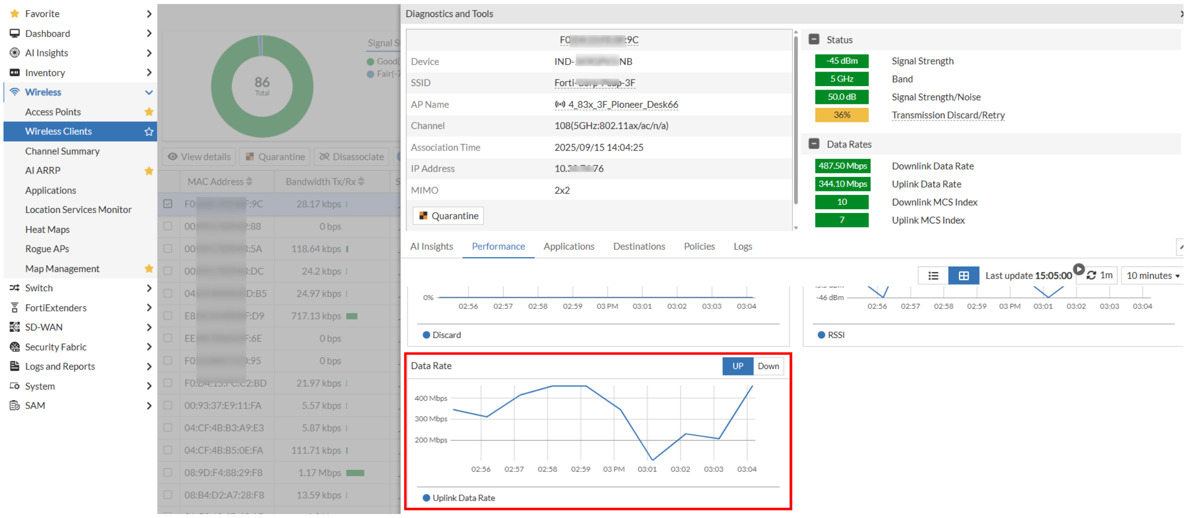
Data Rates

487.50 Mbps	Downlink Data Rate
344.10 Mbps	Uplink Data Rate
10	Downlink MCS Index
7	Uplink MCS Index

Last update **15:05:00**

You can click on any point in the chart to see detailed information like **Timestamp**, **If Index**, **RSSI**, **Tx Data Rate**, and **Rx Data Rate**.

- **Data Rate Chart**: This chart shows the trend of data transmission speeds in both uplink (from the client to the access point) and downlink (from the access point to the client) directions for a client. You can view either of these trends at a time. The speeds are measured in Mbps (Megabits per second).



F0[redacted]:9C

Device	IND-[redacted]NB
SSID	Forti-[redacted]-3F
AP Name	4_83x_3F_Pioneer_Desk66
Channel	108(5GHz:802.11ax/ac/n/a)
Association Time	2025/09/15 14:04:25
IP Address	10.[redacted]76
MIMO	2x2

Status

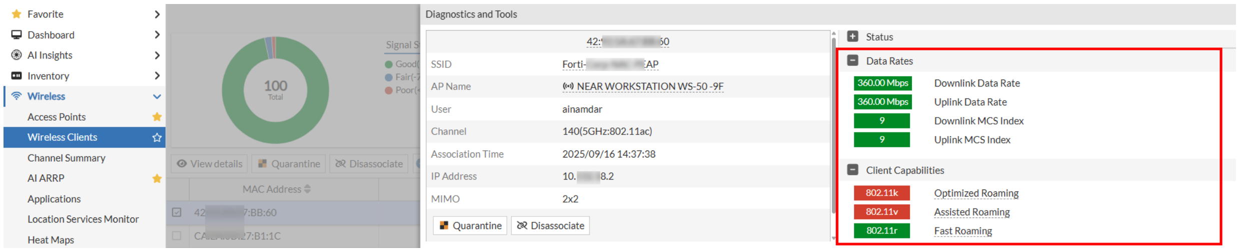
-45 dBm	Signal Strength
5 GHz	Band
50.0 dB	Signal Strength/Noise
36%	Transmission Discard/Retry

Data Rates

487.50 Mbps	Downlink Data Rate
344.10 Mbps	Uplink Data Rate
10	Downlink MCS Index
7	Uplink MCS Index

Similar to the RSSI chart, clicking on any point provides a detailed information like **Timestamp**, **If Index**, **Tx Data Rate**, and **Rx Data Rate**.

Expand Section



42:[redacted]60

SSID	Forti-[redacted]AP
AP Name	NEAR WORKSTATION WS-50 -9F
User	ainamdar
Channel	140(5GHz:802.11ac)
Association Time	2025/09/16 14:37:38
IP Address	10.[redacted]8.2
MIMO	2x2

Status

Data Rates

360.00 Mbps	Downlink Data Rate
360.00 Mbps	Uplink Data Rate
9	Downlink MCS Index
9	Uplink MCS Index

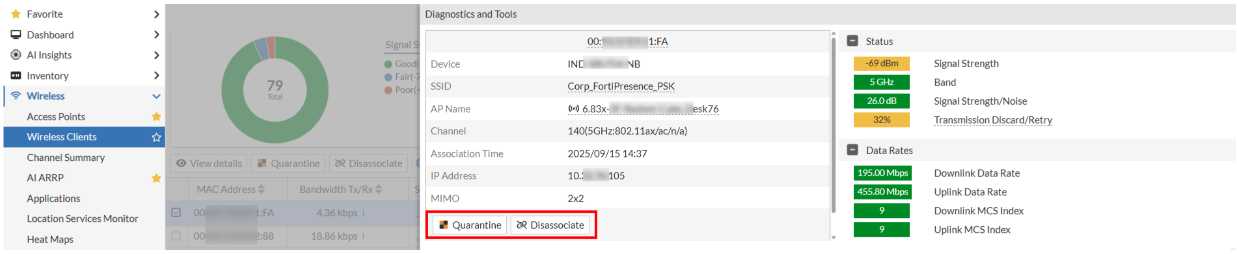
Client Capabilities

802.11k	Optimized Roaming
802.11v	Assisted Roaming
802.11r	Fast Roaming

The expanded section now includes:

- **Data Rates**: A summary of key data rate metrics, including Downlink and Uplink Data Rates, and their corresponding MCS (Modulation and Coding Scheme) Indexes.
- **Client Capabilities**: Displays client status for Optimized Roaming, Fast Roaming, and Assisted Roaming. The capability is shown in green if it is supported and red if it is not supported.
  A **Client Connectivity** widget is also introduced providing an overview of the connection health of wireless clients. See Wireless Dashboard.

New Action Buttons



00:[redacted]1:FA

Device	IND[redacted]NB
SSID	Corp_FortiPresence_PSK
AP Name	6.83x-[redacted]esk76
Channel	140(5GHz:802.11ax/ac/n/a)
Association Time	2025/09/15 14:37
IP Address	10.[redacted]105
MIMO	2x2

Status

-69 dBm	Signal Strength
5 GHz	Band
26.0 dB	Signal Strength/Noise
32%	Transmission Discard/Retry

Data Rates

195.00 Mbps	Downlink Data Rate
455.80 Mbps	Uplink Data Rate
9	Downlink MCS Index
9	Uplink MCS Index

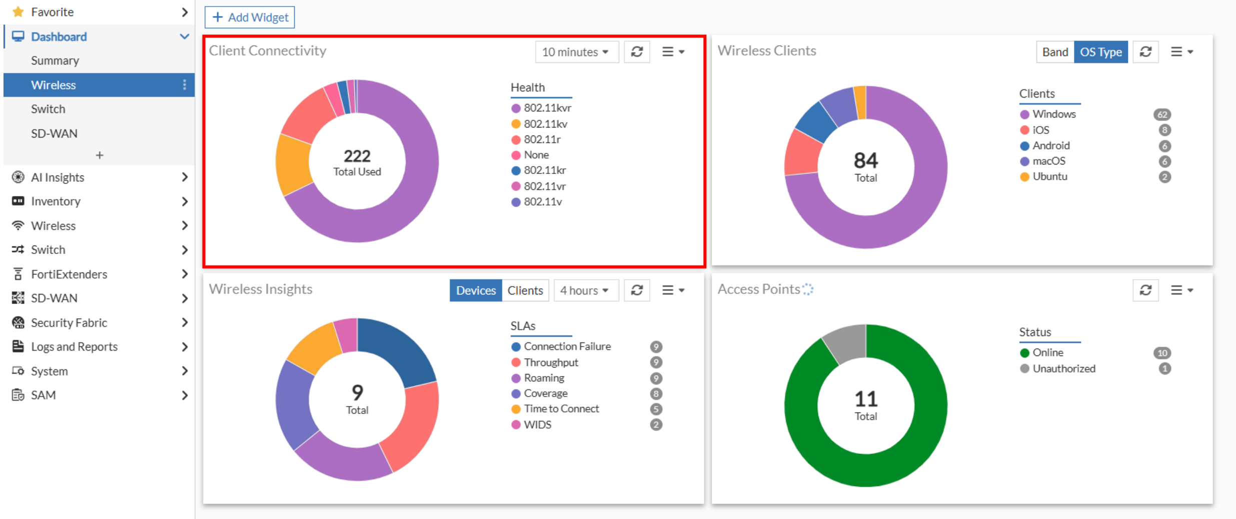
The Diagnostics and Tools window also includes new buttons to manage wireless clients:

- **Quarantine**: This button adds the device MAC address to a quarantine list, allowing FortiGate to apply security policies that block all or specific network access for that device.
    - This button is available for both currently and previously connected clients.
    - If a client is not quarantined, the button will show **Quarantine.** If it is already quarantined, the button will change to **Unquarantine.**
    - Quarantined clients are also visually highlighted on the main **Wireless Clients** window (**Wireless** > **Wireless Clients**).
- **Disassociate**: This button immediately disconnects a client from its access point.
    - This option is only available when the time range is set to **Now**.

Wireless Dashboard

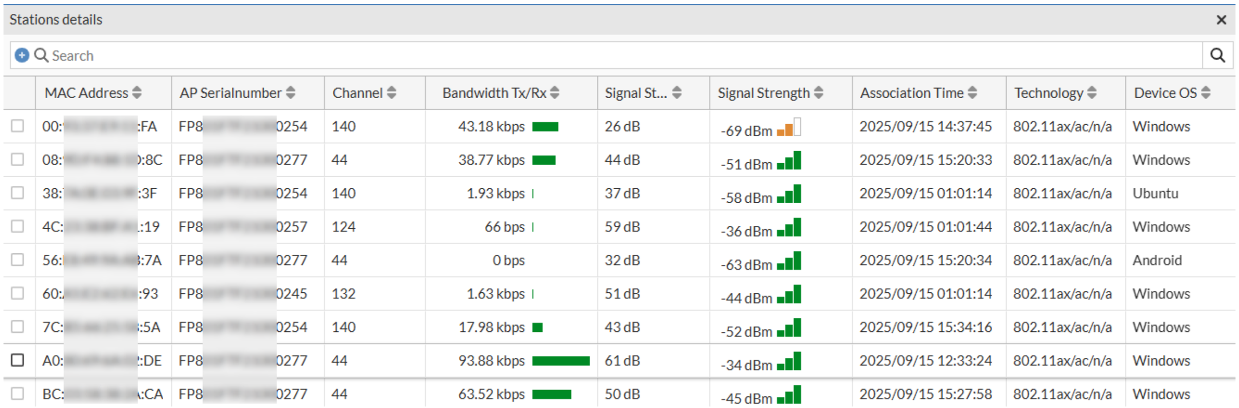
A **Client Connectivity** widget is introduced in the **Wireless** dashboard to provide a quick and informative overview of the connection health of wireless clients over a specific time period (in this case, 10 minutes). The widget represents the total number of clients connected during that time, categorized by their connection status or capabilities.

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



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

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

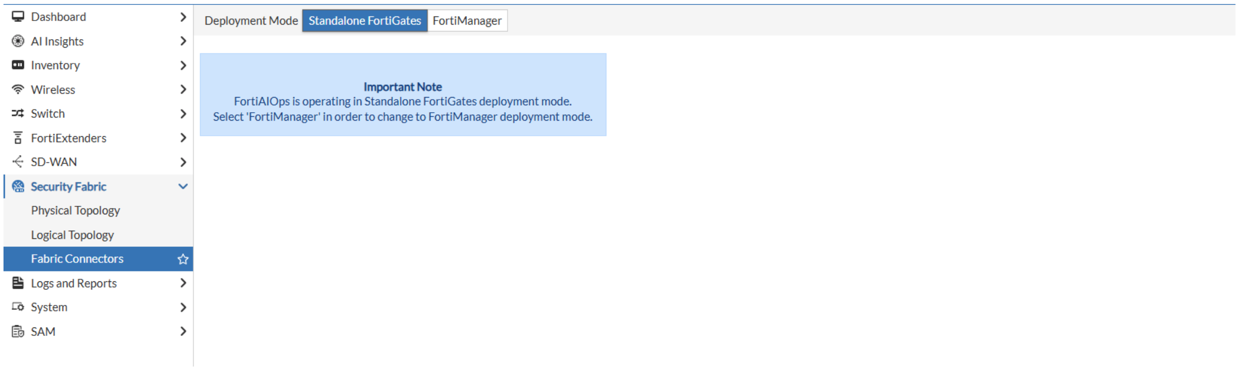


	MAC Address	AP Serialnumber	Channel	Bandwidth Tx/Rx	Signal St...	Signal Strength	Association Time	Technology	Device OS
☐	00:[redacted]:FA	FP8[redacted]0254	140	43.18 kbps	26 dB	-69 dBm	2025/09/15 14:37:45	802.11ax/ac/n/a	Windows
☐	08:[redacted]:8C	FP8[redacted]0277	44	38.77 kbps	44 dB	-51 dBm	2025/09/15 15:20:33	802.11ax/ac/n/a	Windows
☐	38:[redacted]:3F	FP8[redacted]0254	140	1.93 kbps	37 dB	-58 dBm	2025/09/15 01:01:14	802.11ax/ac/n/a	Ubuntu
☐	4C:[redacted]:19	FP8[redacted]0257	124	66 bps	59 dB	-36 dBm	2025/09/15 01:01:44	802.11ax/ac/n/a	Windows
☐	56:[redacted]:7A	FP8[redacted]0277	44	0 bps	32 dB	-63 dBm	2025/09/15 15:20:34	802.11ax/ac/n/a	Android
☐	60:[redacted]:93	FP8[redacted]0245	132	1.63 kbps	51 dB	-44 dBm	2025/09/15 01:01:14	802.11ax/ac/n/a	Windows
☐	7C:[redacted]:5A	FP8[redacted]0254	140	17.98 kbps	43 dB	-52 dBm	2025/09/15 15:34:16	802.11ax/ac/n/a	Windows
☐	A0:[redacted]:DE	FP8[redacted]0277	44	93.88 kbps	61 dB	-34 dBm	2025/09/15 12:33:24	802.11ax/ac/n/a	Windows
☐	BC:[redacted]:CA	FP8[redacted]0277	44	63.52 kbps	50 dB	-45 dBm	2025/09/15 15:27:58	802.11ax/ac/n/a	Windows

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

Fabric Connectors: Deployment Mode Selection

A new **Fabric Connectors** window is available under **Security Fabric** to manage the **Deployment Mode**. This setting determines how FortiAIOps discovers and communicates with network devices.



Deployment Mode: Standalone FortiGates

Important Note
FortiAIOps is operating in Standalone FortiGates deployment mode.
Select 'FortiManager' in order to change to FortiManager deployment mode.

Two deployment modes are available:

Standalone FortiGates

FortiAIOps operates independently and establishes direct connections to individual FortiGate devices.

Note: This is the default configuration.

FortiManager

A centralized mode where FortiAIOps connects via the FortiManager Fabric Connector instead of communicating with devices individually.

Note: This mode requires FortiManager version 7.6.7 or 8.0.0, which will be released at a later date.

Packet Capture Analysis using FortiAI (Generative AI Assistant)

FortiAI now supports comprehensive packet capture (PCAP) management, allowing users to analyze network traffic directly through the FortiAI interface. This feature includes two main capabilities:

PCAP Upload and Analysis

You can now upload existing PCAP files for immediate AI analysis. Once uploaded, you can query FortiAI regarding the traffic, such as identifying DHCP issues, troubleshooting connectivity for specific client MAC addresses, or counting probe requests.

Triggering a Live Packet Capture

You can also initiate a packet capture on a specific FortiGate interface. A sample command to initiate the packet capture is as follows:

```
trigger packet capture on <interface name> at <FGT name>
```

Upon completion, a download link for the PCAP file is provided which can be downloaded for further analysis.

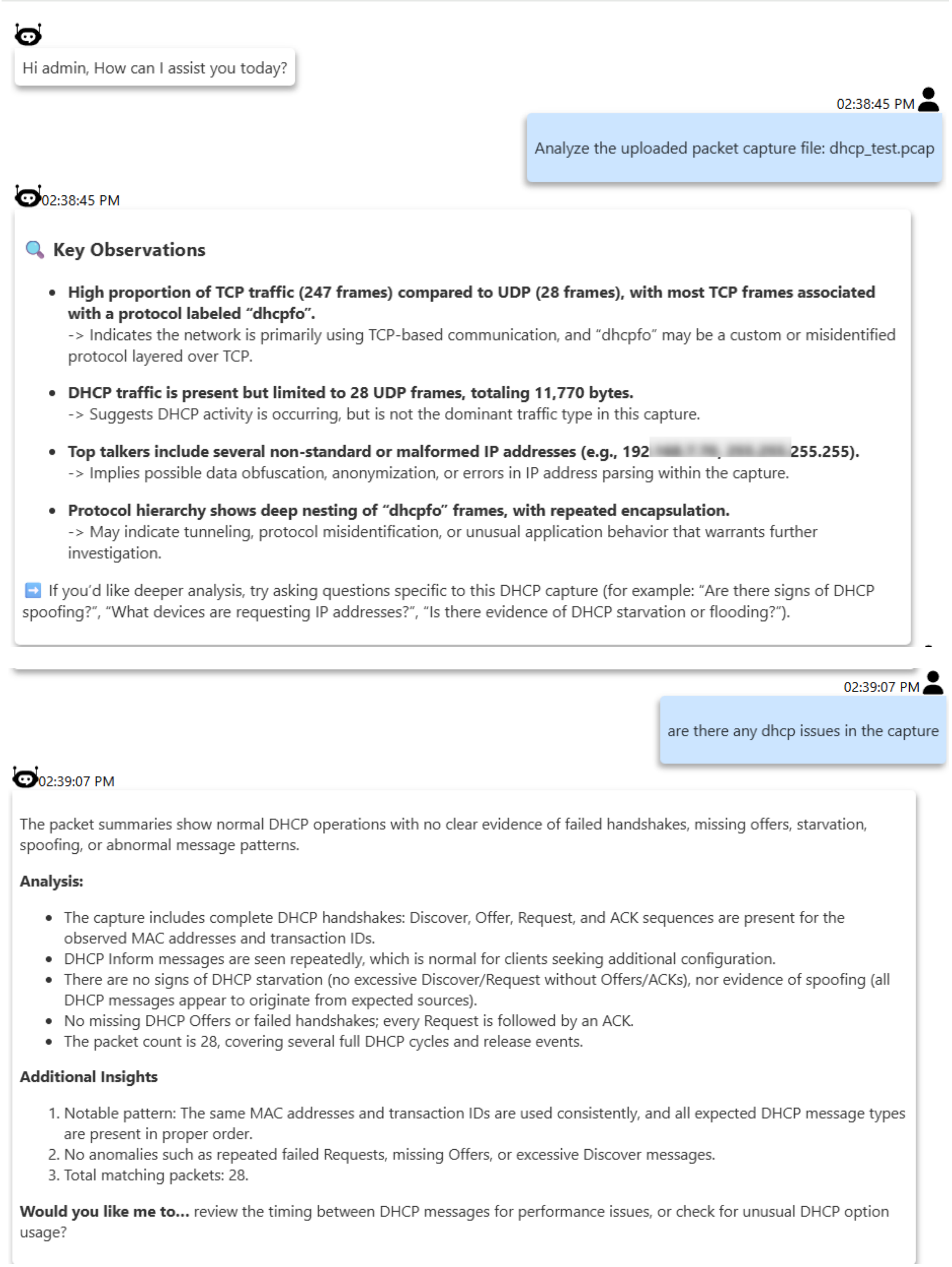
Example Tasks

The following are some example tasks for reference:

Example 1: Analyze PCAP file

You can upload existing PCAP files for AI analysis. Once uploaded, you can ask questions regarding the traffic, such as identifying DHCP issues, troubleshooting connectivity for specific client MAC addresses, counting probe requests, and so on.

Prompt: Analyze the uploaded packet capture file: <file_name>



Hi admin, How can I assist you today?

02:38:45 PM

Analyze the uploaded packet capture file: dhcp_test.pcap

02:38:45 PM

🔍 Key Observations

- **High proportion of TCP traffic (247 frames) compared to UDP (28 frames), with most TCP frames associated with a protocol labeled "dhcpfo".**
  -> Indicates the network is primarily using TCP-based communication, and "dhcpfo" may be a custom or misidentified protocol layered over TCP.
- **DHCP traffic is present but limited to 28 UDP frames, totaling 11,770 bytes.**
  -> Suggests DHCP activity is occurring, but is not the dominant traffic type in this capture.
- **Top talkers include several non-standard or malformed IP addresses (e.g., 192[redacted], [redacted]255.255).**
  -> Implies possible data obfuscation, anonymization, or errors in IP address parsing within the capture.
- **Protocol hierarchy shows deep nesting of "dhcpfo" frames, with repeated encapsulation.**
  -> May indicate tunneling, protocol misidentification, or unusual application behavior that warrants further investigation.

➡️ If you'd like deeper analysis, try asking questions specific to this DHCP capture (for example: "Are there signs of DHCP spoofing?", "What devices are requesting IP addresses?", "Is there evidence of DHCP starvation or flooding?").

02:39:07 PM

are there any dhcp issues in the capture

02:39:07 PM

The packet summaries show normal DHCP operations with no clear evidence of failed handshakes, missing offers, starvation, spoofing, or abnormal message patterns.

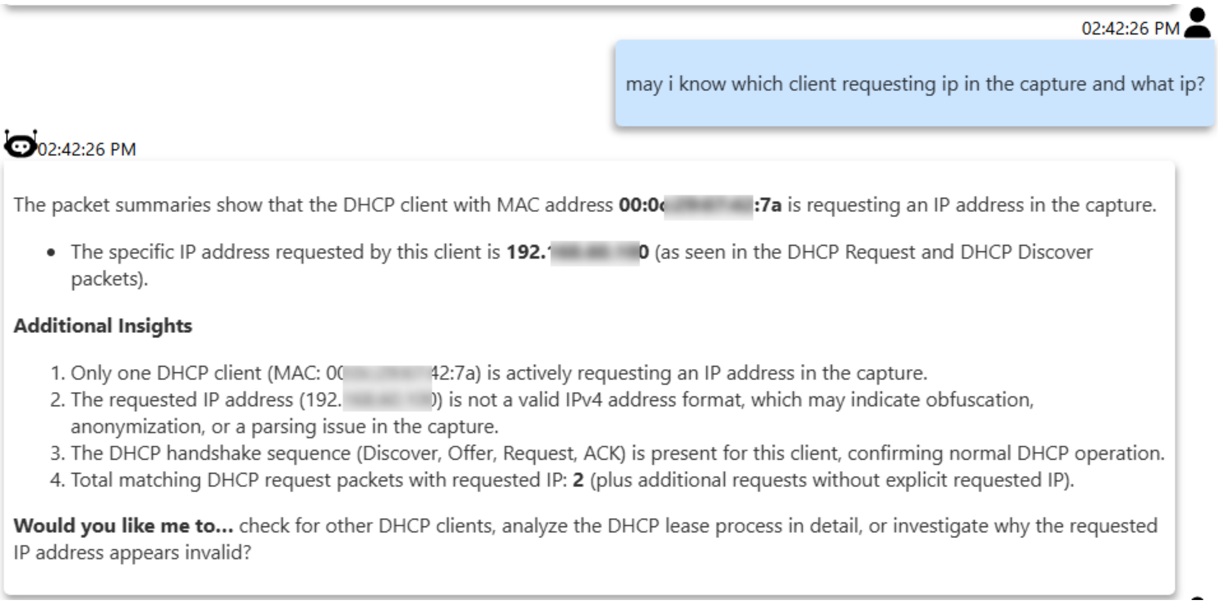
Analysis:

- The capture includes complete DHCP handshakes: Discover, Offer, Request, and ACK sequences are present for the observed MAC addresses and transaction IDs.
- DHCP Inform messages are seen repeatedly, which is normal for clients seeking additional configuration.
- There are no signs of DHCP starvation (no excessive Discover/Request without Offers/ACKs), nor evidence of spoofing (all DHCP messages appear to originate from expected sources).
- No missing DHCP Offers or failed handshakes; every Request is followed by an ACK.
- The packet count is 28, covering several full DHCP cycles and release events.

Additional Insights

1. Notable pattern: The same MAC addresses and transaction IDs are used consistently, and all expected DHCP message types are present in proper order.
2. No anomalies such as repeated failed Requests, missing Offers, or excessive Discover messages.
3. Total matching packets: 28.

Would you like me to... review the timing between DHCP messages for performance issues, or check for unusual DHCP option usage?



02:42:26 PM

may i know which client requesting ip in the capture and what ip?

02:42:26 PM

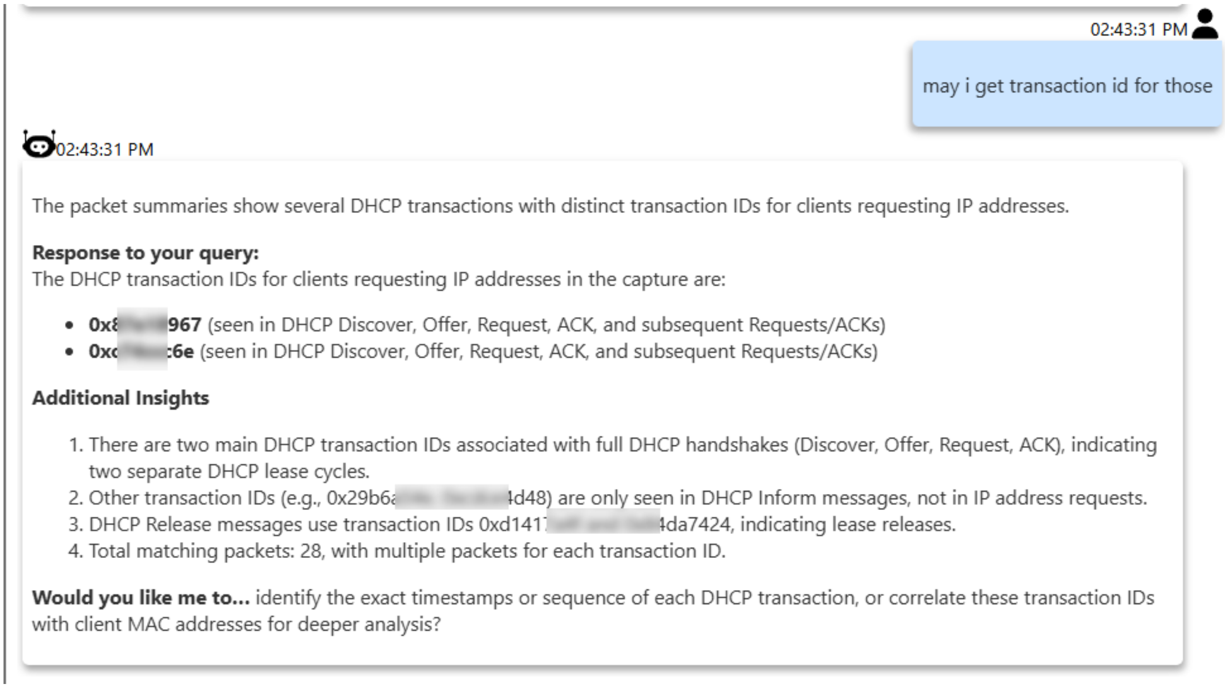
The packet summaries show that the DHCP client with MAC address **00:0[redacted]:7a** is requesting an IP address in the capture.

- The specific IP address requested by this client is **192.[redacted]0** (as seen in the DHCP Request and DHCP Discover packets).

Additional Insights

1. Only one DHCP client (MAC: 00[redacted]42:7a) is actively requesting an IP address in the capture.
2. The requested IP address (192.[redacted]) is not a valid IPv4 address format, which may indicate obfuscation, anonymization, or a parsing issue in the capture.
3. The DHCP handshake sequence (Discover, Offer, Request, ACK) is present for this client, confirming normal DHCP operation.
4. Total matching DHCP request packets with requested IP: **2** (plus additional requests without explicit requested IP).

Would you like me to... check for other DHCP clients, analyze the DHCP lease process in detail, or investigate why the requested IP address appears invalid?



02:43:31 PM

may i get transaction id for those

02:43:31 PM

The packet summaries show several DHCP transactions with distinct transaction IDs for clients requesting IP addresses.

Response to your query:
The DHCP transaction IDs for clients requesting IP addresses in the capture are:

- **0x8[redacted]967** (seen in DHCP Discover, Offer, Request, ACK, and subsequent Requests/ACKs)
- **0xc[redacted]:6e** (seen in DHCP Discover, Offer, Request, ACK, and subsequent Requests/ACKs)

Additional Insights

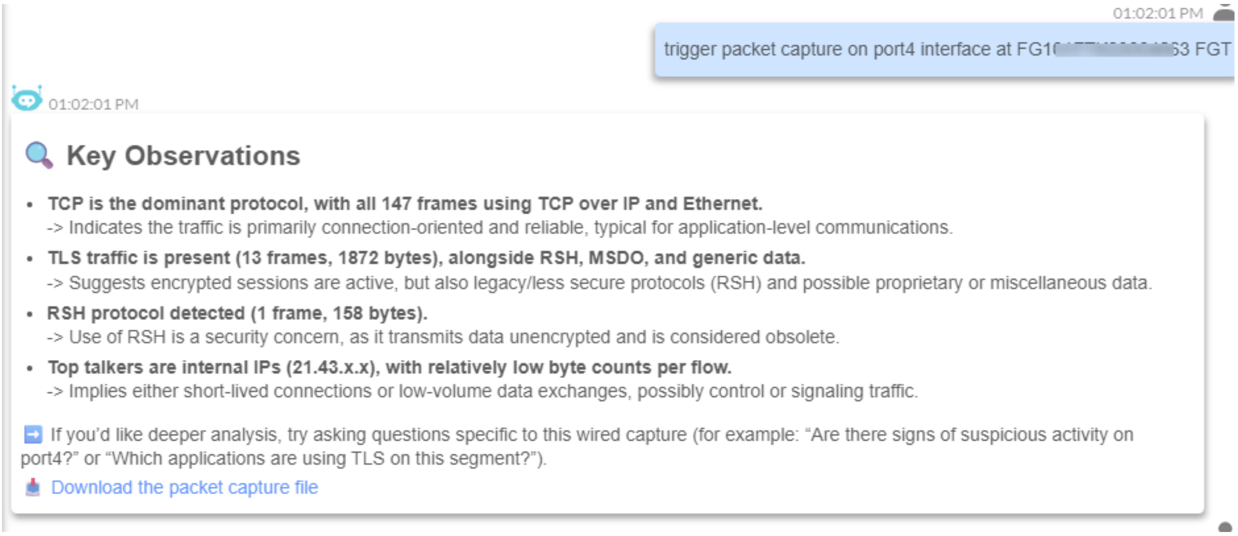
1. There are two main DHCP transaction IDs associated with full DHCP handshakes (Discover, Offer, Request, ACK), indicating two separate DHCP lease cycles.
2. Other transaction IDs (e.g., 0x29b6[redacted]4d48) are only seen in DHCP Inform messages, not in IP address requests.
3. DHCP Release messages use transaction IDs 0xd141[redacted]4da7424, indicating lease releases.
4. Total matching packets: 28, with multiple packets for each transaction ID.

Would you like me to... identify the exact timestamps or sequence of each DHCP transaction, or correlate these transaction IDs with client MAC addresses for deeper analysis?

Example 2: Trigger Packet Capture

You can initiate a packet capture on a specific FortiGate interface. The PCAP file thus generated can be downloaded for further analysis.

Prompt: trigger packet capture on <interface name> at <FGT name>



01:02:01 PM

trigger packet capture on port4 interface at FG1[redacted]63 FGT

01:02:01 PM

🔍 Key Observations

- **TCP is the dominant protocol, with all 147 frames using TCP over IP and Ethernet.**
  -> Indicates the traffic is primarily connection-oriented and reliable, typical for application-level communications.
- **TLS traffic is present (13 frames, 1872 bytes), alongside RSH, MSDO, and generic data.**
  -> Suggests encrypted sessions are active, but also legacy/less secure protocols (RSH) and possible proprietary or miscellaneous data.
- **RSH protocol detected (1 frame, 158 bytes).**
  -> Use of RSH is a security concern, as it transmits data unencrypted and is considered obsolete.
- **Top talkers are internal IPs (21.43.x.x), with relatively low byte counts per flow.**
  -> Implies either short-lived connections or low-volume data exchanges, possibly control or signaling traffic.

➡️ If you'd like deeper analysis, try asking questions specific to this wired capture (for example: “Are there signs of suspicious activity on port4?” or “Which applications are using TLS on this segment?”).

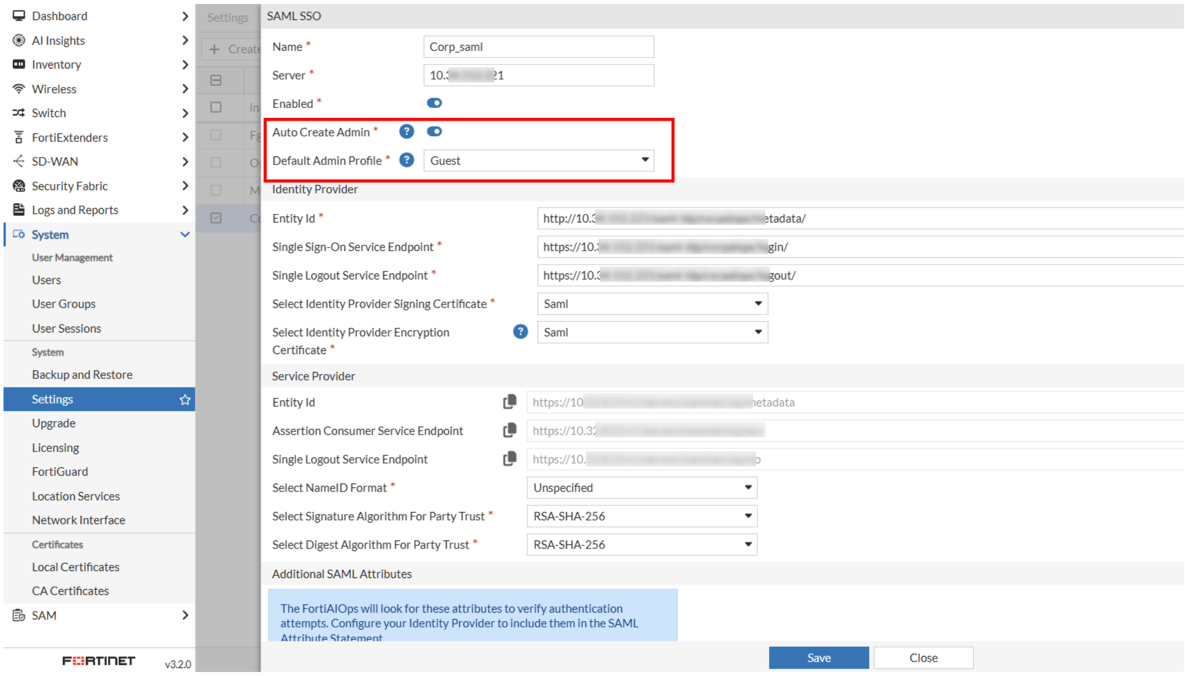
📥 Download the packet capture file

Remote Authentication

FortiAIOps now supports the automatic provisioning of admin accounts upon successful SAML authentication. This release introduces the **Auto Create Admin** setting, which requires the selection of a **Default Admin Profile**. When an SSO user logs in, the system automatically generates an admin account with the assigned profile permissions. These accounts persist in the database indefinitely. They are not removed upon logout and must be deleted manually if no longer needed.

To enable Auto Create Admin:

1. Navigate to **System** > **Settings** > **Authentication Servers** tab.
2. Create or edit **SAML SSO** or **Microsoft ADFS SAML IDP** server type.



SAML SSO

Name * Corp_saml

Server * 10.[redacted]1

Enabled * ●

Auto Create Admin * ●

Default Admin Profile * Guest

Identity Provider

Entity Id * http://10.[redacted]etadata/

Single Sign-On Service Endpoint * https://10.[redacted]gin/

Single Logout Service Endpoint * https://10.[redacted]gout/

Select Identity Provider Signing Certificate * Saml

Select Identity Provider Encryption Certificate * Saml

Service Provider

Entity Id https://10[redacted]netadata

Assertion Consumer Service Endpoint https://10.3[redacted]

Single Logout Service Endpoint https://10.[redacted]o

Select NameID Format * Unspecified

Select Signature Algorithm For Party Trust * RSA-SHA-256

Select Digest Algorithm For Party Trust * RSA-SHA-256

Additional SAML Attributes

The FortiAIOps will look for these attributes to verify authentication attempts. Configure your Identity Provider to include them in the SAML Attribute Statement

3. Enable Auto Create Admin using the toggle button.
4. Select the Default Admin Profile from the drop down.
5. Click **Save**.

Dashboard Filter Persistence

This release introduces persistence for dashboard customizations, significantly improving workflow efficiency. All customizations made to widgets such as specific data filters, window resizing, and layout positioning are now automatically saved to the individual user profile.

This ensures that your personalized dashboard state is preserved not just across page reloads and logouts, but also when switching between browsers or navigating different ADOMs. These configurations are stored at the user level and your preferred view remains unchanged and is never overwritten by global system changes or the activities of other administrators.

www.fortinet.com

Copyright© 2026 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.