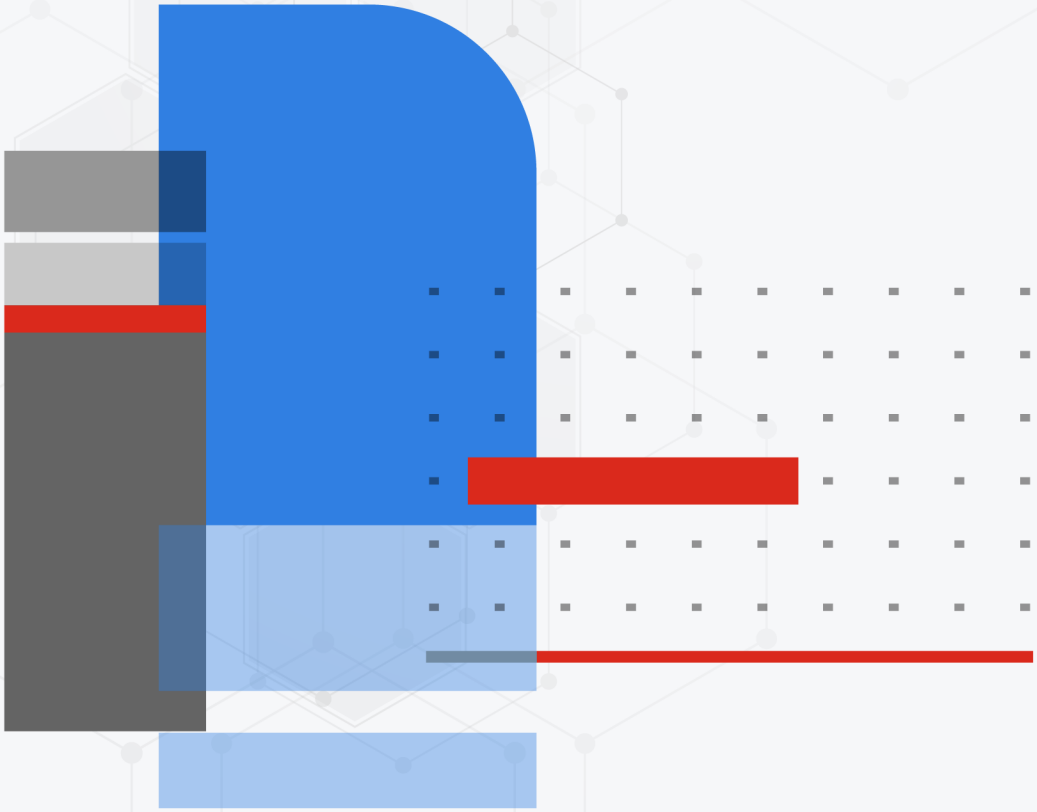
New Features

FortiAIOps 3.4.0



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

May 08, 2026
FortiAIOps 3.4.0 New Features
83-340-1277709-20260508

TABLE OF CONTENTS

Change log

Date	Change description
2026-05-08	FortiAIOps release 3.4.0 document.

About the Release

This release introduces the following new features:

- Network Assurance Dashboard
- Wireless Client Roaming
- FortiAIOps 2000G Hardware Support
- FortiAI Tokens

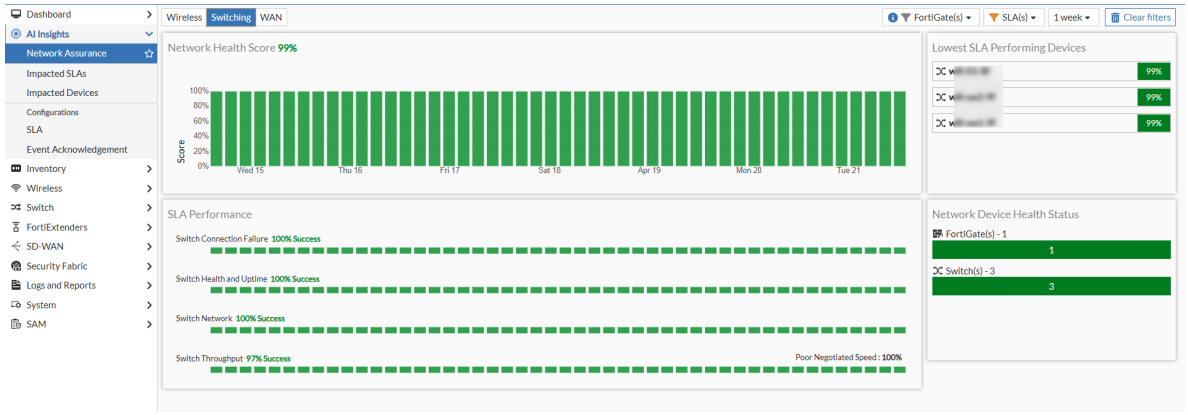
Network Assurance Dashboard

This release introduces a new **Network Assurance Dashboard** under the **AI Insights** menu. The **Network Assurance Dashboard** provides a centralized graphical interface to monitor the SLA performance and overall network health status of all devices within a selected ADOM. This feature allows administrators to evaluate SLA performance comprehensively or drill down into specific devices, ensuring high availability and optimized performance across the network.

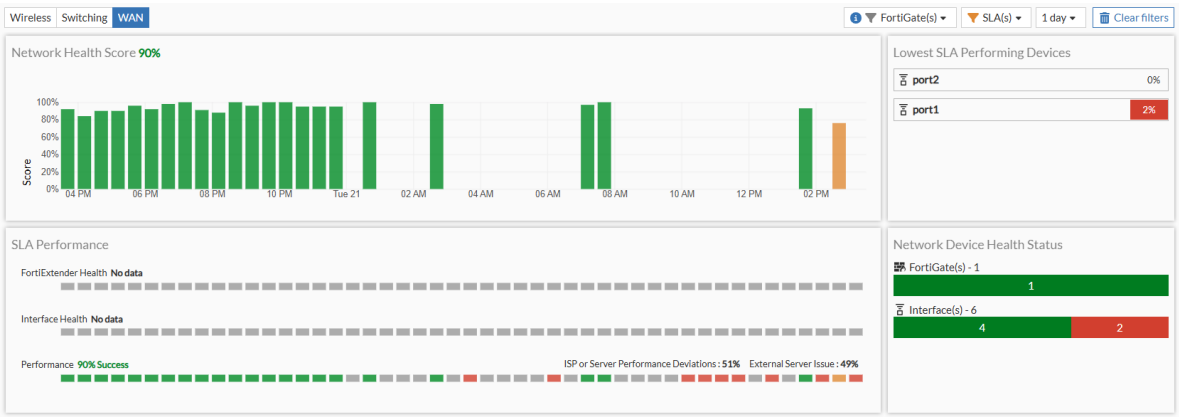
The dashboard evaluates SLA performance across:

- **Wireless**

- **Switching**



- **WAN**



Navigate to the relevant sections using the **Wireless**, **Switching**, or **WAN** tabs.

Filtering Your View

You can narrow down the dashboard data using the filters located at the top of the page:

- FortiGate(s): Filter by specific FortiGates within the chosen ADOM.
- Duration: Choose a predefined time-frame (1 hour, 4 hours, 6 hours, 12 hours, 1 day, or 1 week) or set a custom date range up to 1 week.
- SLA(s): Use the drop down to view data for specific SLA(s).

Scoring and Color Coding

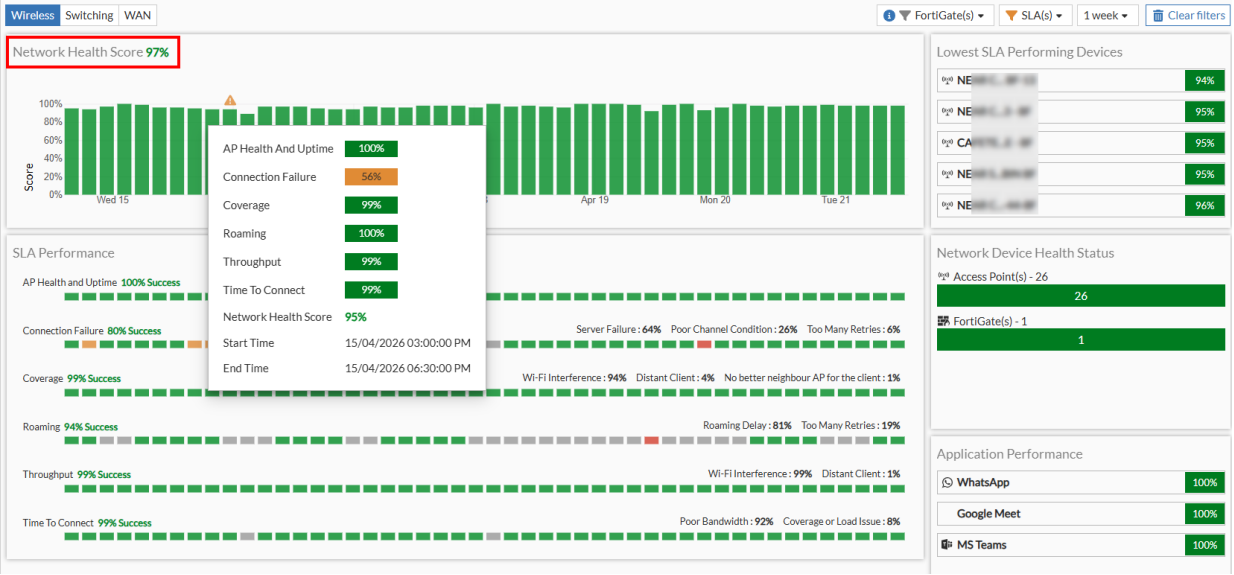
The dashboard calculates a score for your network and individual SLAs and represents the calculated scores using the following color thresholds:

- Green: Good
- Yellow: Fair
- Red: Poor
- Grey: No data available

Note: Device scoring information is also available in the device drill-down view.

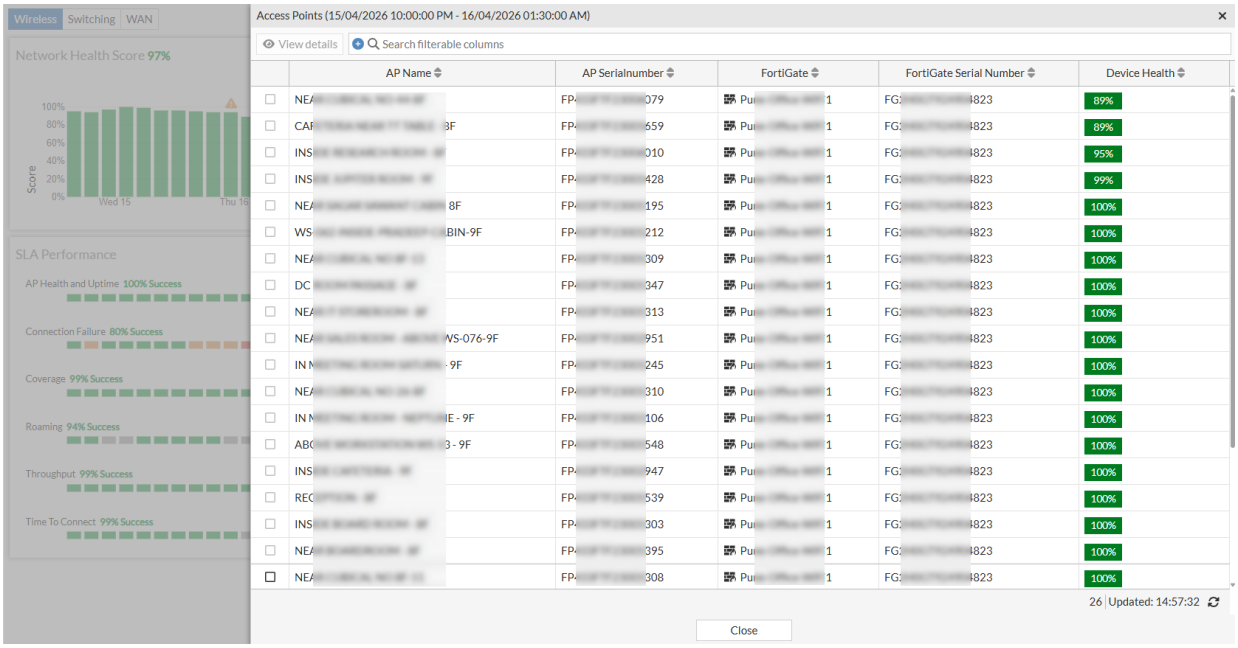
Network Health Score

The **Network Health Score** section displays the overall health of the selected SLAs over a specific time period.

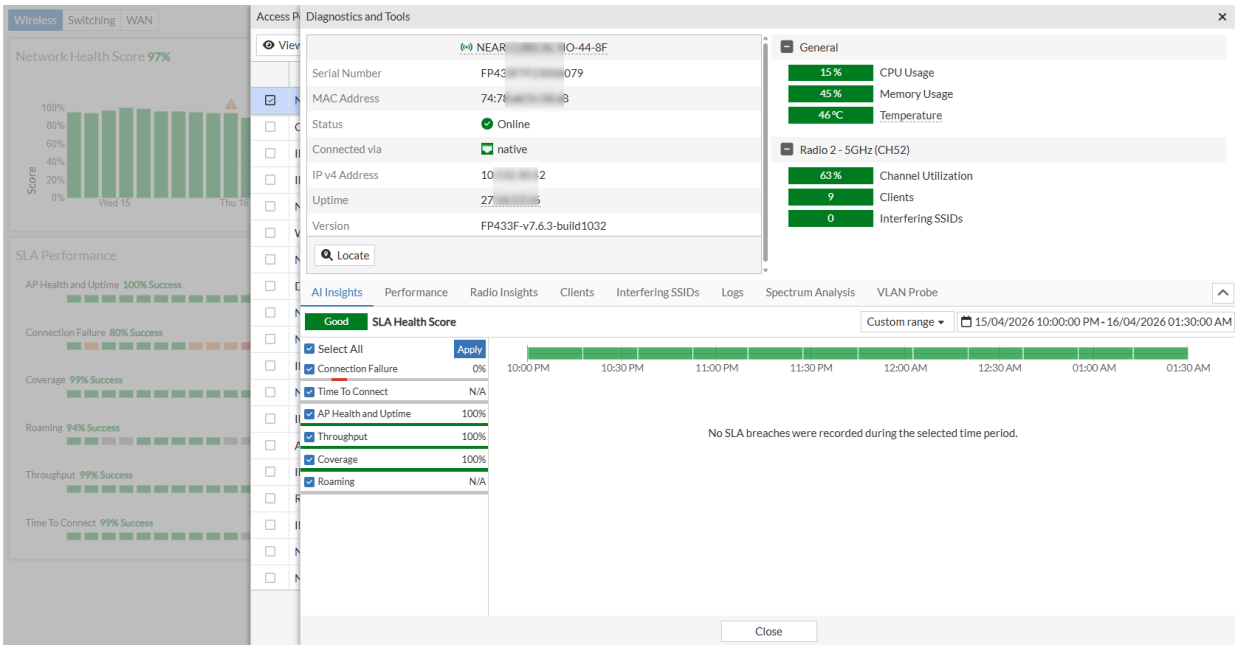


Hovering over a grid provides details of the individual scores for the SLAs during that specific time interval.

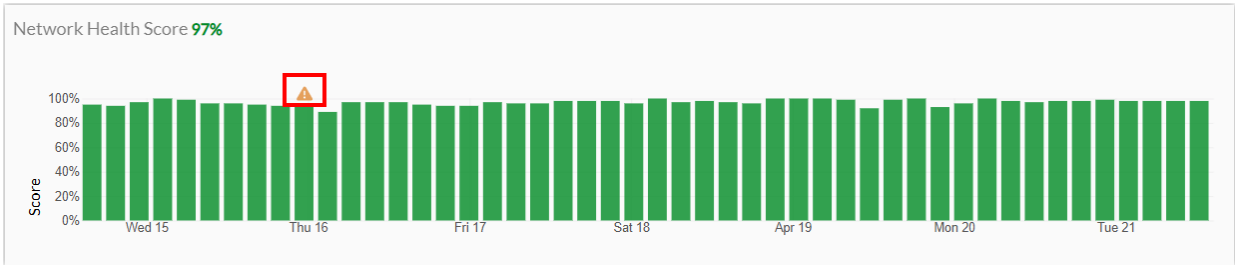
Clicking on a grid opens the **Access Points** pane with details such as AP Name, AP Serial Number, FortiGate, FortiGate Serial Number, and Device Health captured.



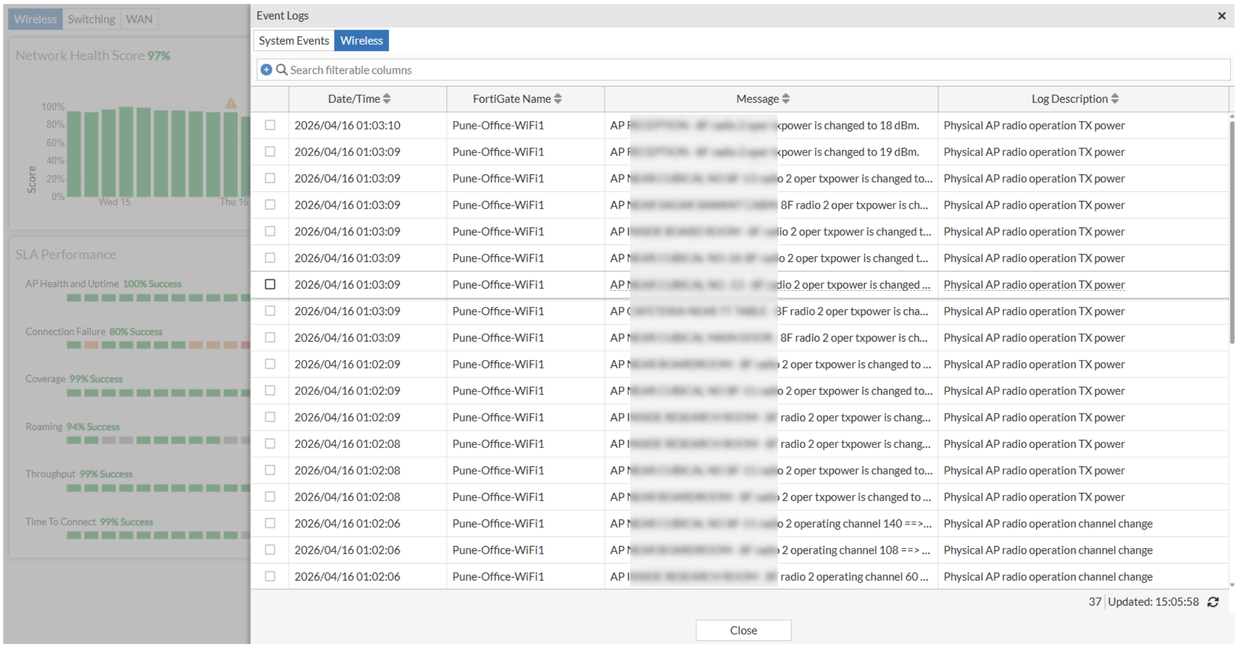
Select an AP and click **View Details** to view the **Diagnostics and Tools** pane for the device.



If a grid has an associated warning symbol, it means that an event (including any system events) was logged during this time interval.

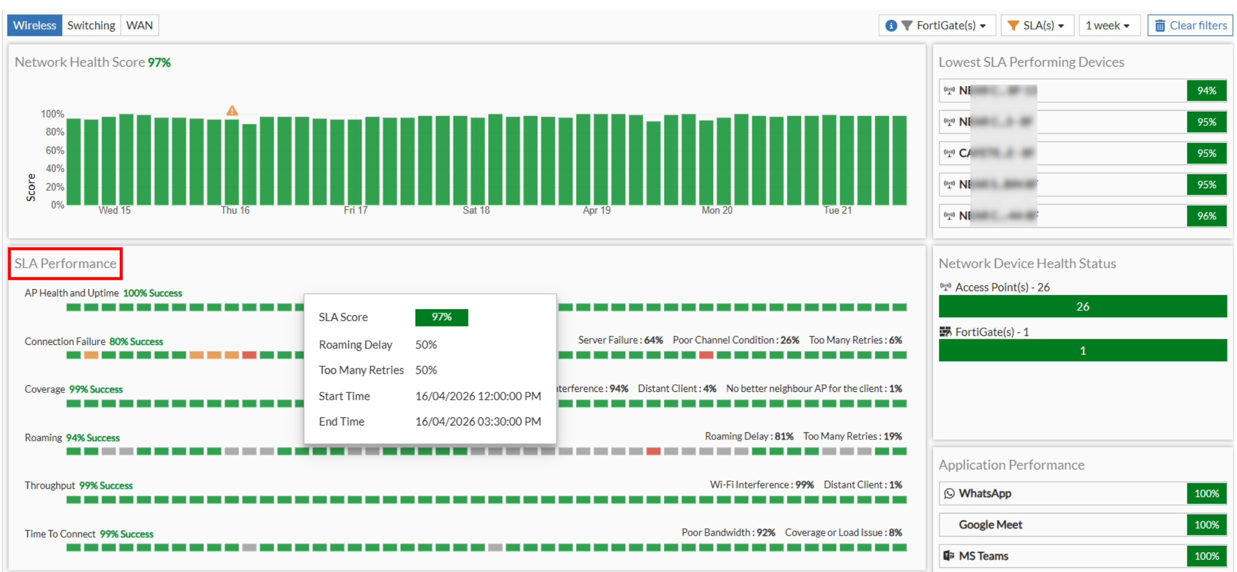


Clicking on the warning symbol opens the **Event Logs** pane displaying any system or device events that are logged. This allows you to easily correlate performance degradation with specific system changes.



SLA Performance

The **SLA Performance** section breaks down performance by individual SLAs for all the selected SLAs over a chosen time period.



For each SLA, the dashboard highlights the top sub-classifiers contributing to impacted events. It displays the exact percentage that each sub-classifier contributes to the total issues for that duration.

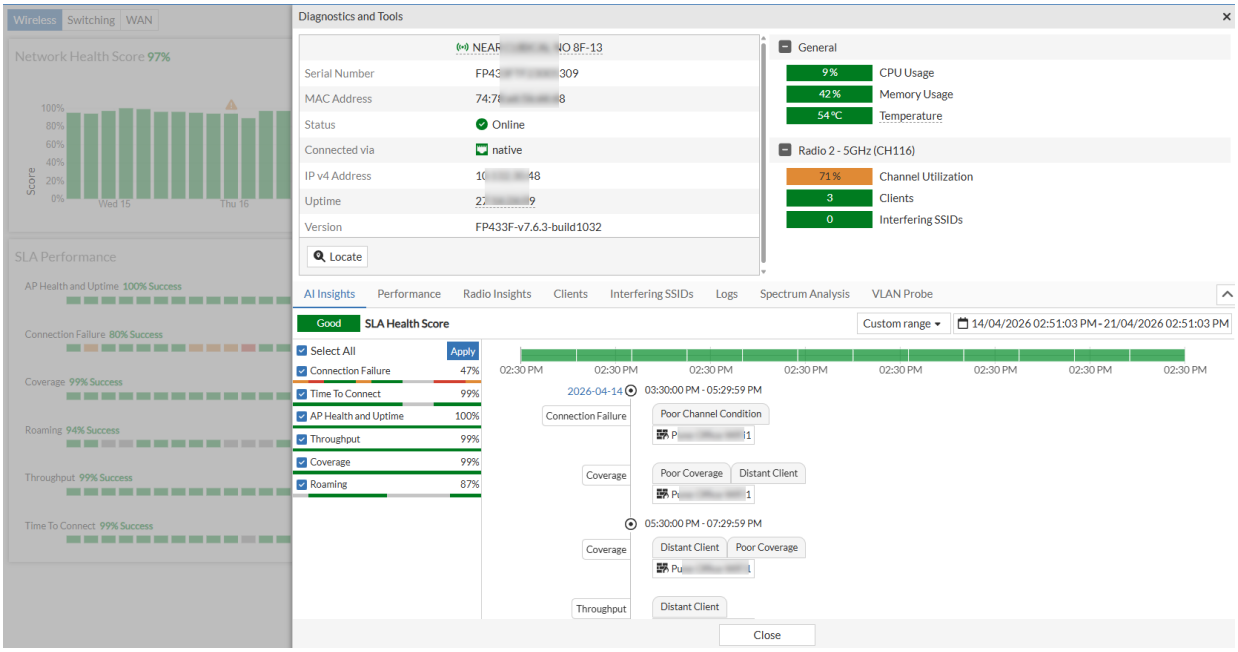
Clicking on the grid opens the **Access Points** pane with more detailed information.

Select an AP and click **View Details** to view the **Diagnostics and Tools** pane for the device.

Lowest SLA Performing Devices

This section lists the top 5 problematic access points with the lowest SLA score during the selected duration. It displays their overall health status (Green / Yellow / Red) based on their individual scores.

Clicking on a device opens the **Diagnostics and Tools** pane for the device.



Network Device Health Status

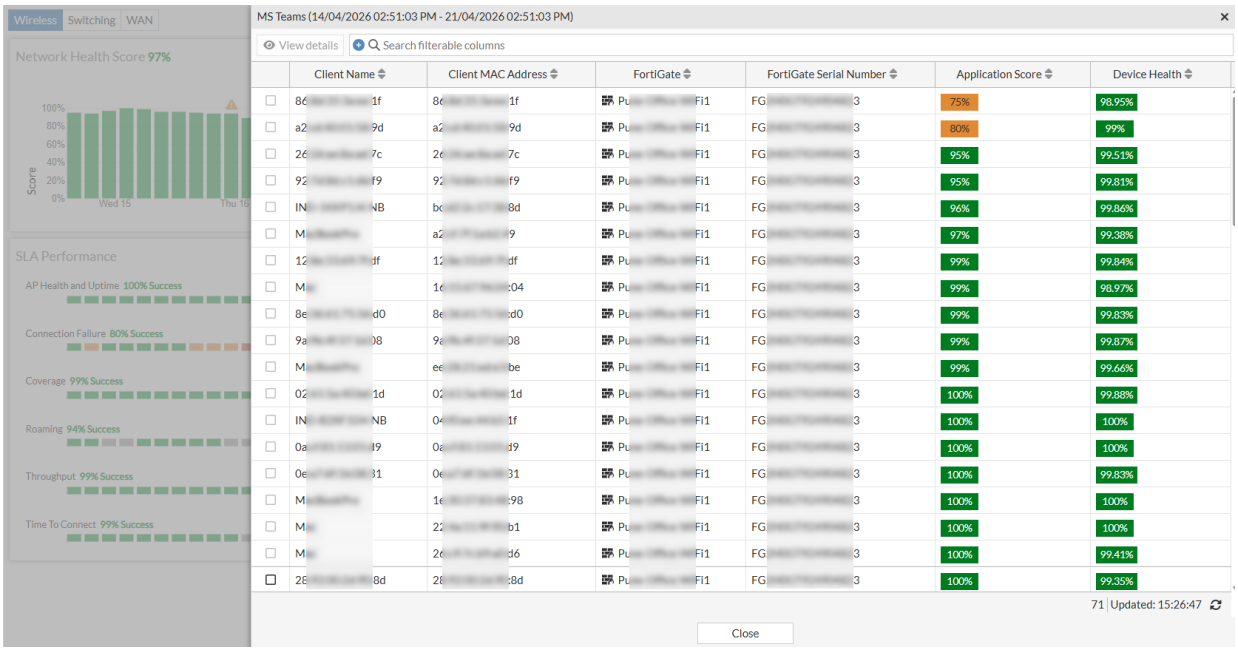
This **Network Device Health Status** section provides a quick summary of device counts within the ADOM and their corresponding health.

Click on a device type to open the details pane with detailed information. Select device and click **View Details** to view the **Diagnostics and Tools** pane for the wireless device.

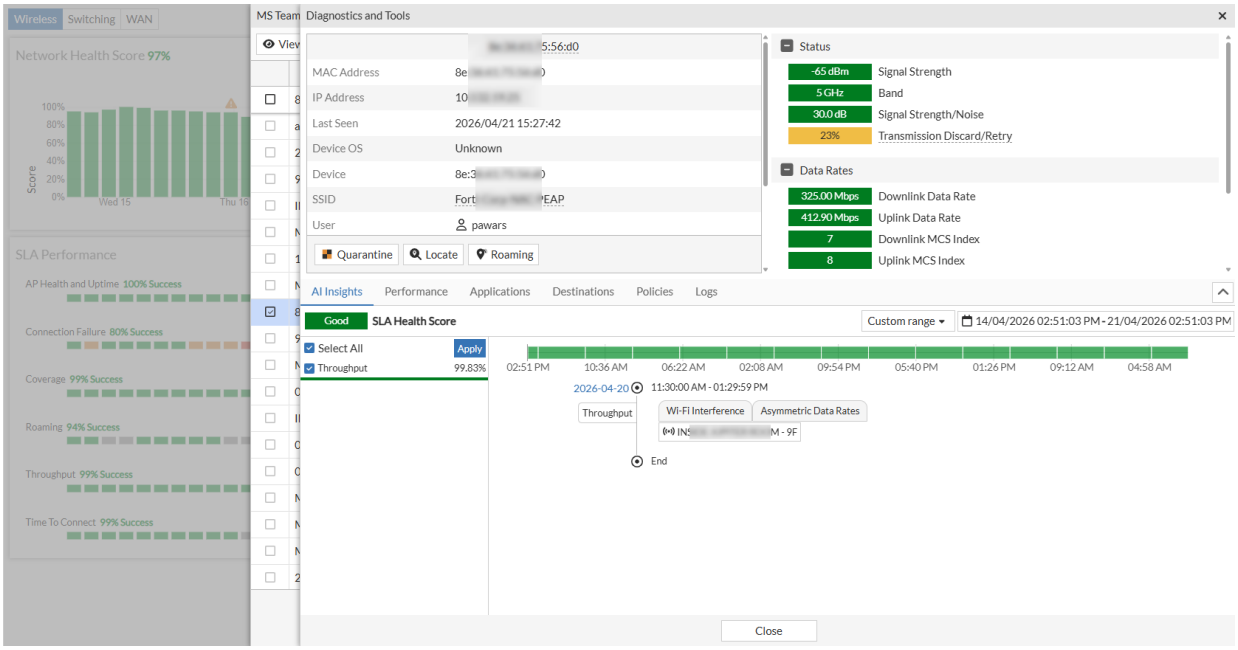
Application Performance

The **Application Performance** section displays all the applications being used along with any performance issues being faced by the applications.

Clicking on an application name opens a pane with the details of clients such as Client Name, Client MAC Address, FortiGate, FortiGate Serial Number, Application Score, and Device Health.



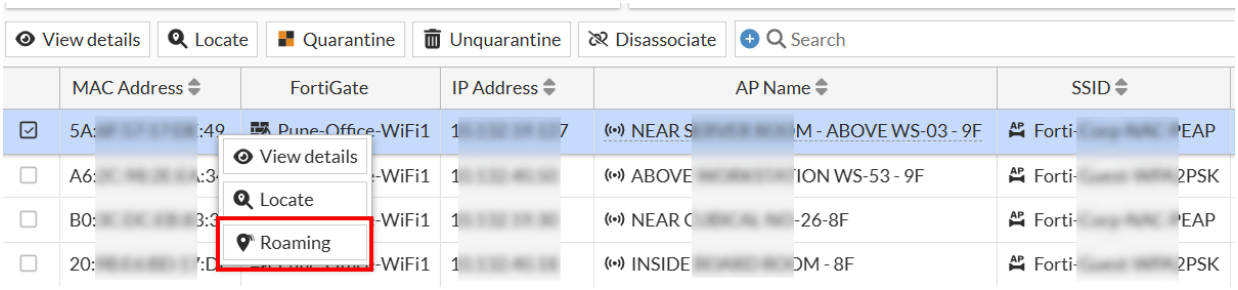
Select a client and click **View Details** to open the **Diagnostics and Tools** pane for the client.



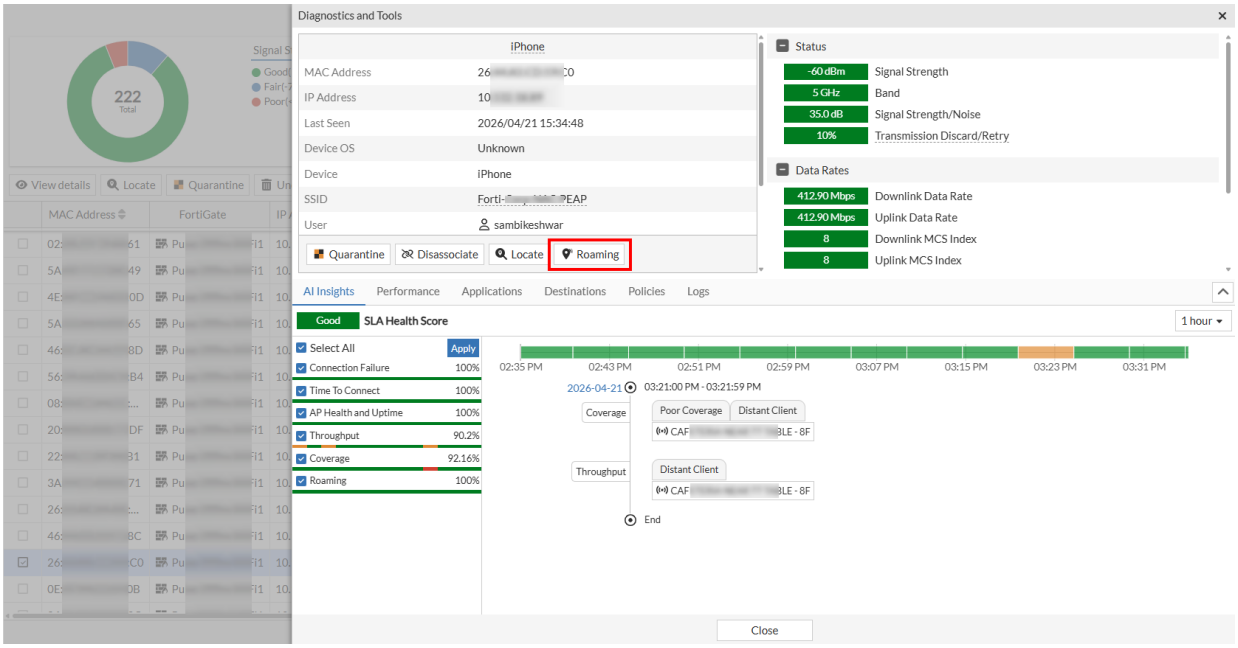
Wireless Client Roaming

This release introduces **Roaming** feature for Wireless Clients. The feature provides a graphical roaming and connectivity experience for administrators to visually track the journey of a wireless client across the network and identify any connectivity issues.

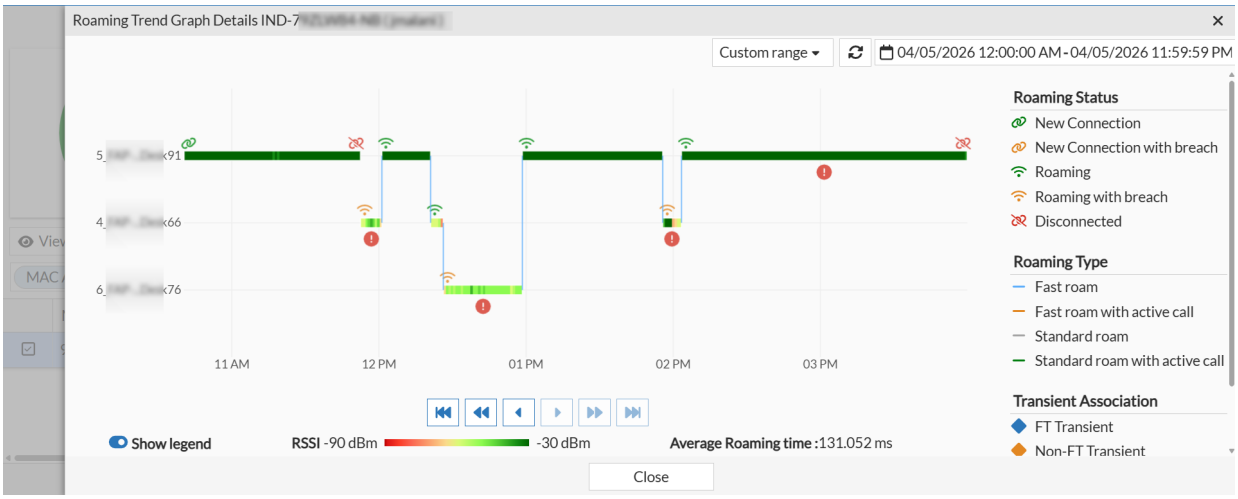
To view the roaming history of a wireless client, navigate to **Wireless** > **Wireless Clients**. Select a wireless device, right click and select **Roaming**.



Alternatively, you can also select a specific client and click **View Details** to open the **Diagnostics and Tools** pane. Click the **Roaming** button.



The **Roaming Trend Graph Details** pane displays the roaming history of the client:



Time Range

- The default time range is set to 6 hours. You can select from the following standard intervals: 1 hour, 4 hours, 6 hours, and 1 day.
- A custom time range can be defined to a maximum span of 1 day for any selected date and time.
- When viewing a specific client, you can navigate the timeline to view the Previous or Next 1 hour, 6 hours, or 24 hours.

The timeline provides a graphical representation of the client connectivity with different APs across the chosen time period using the following components:

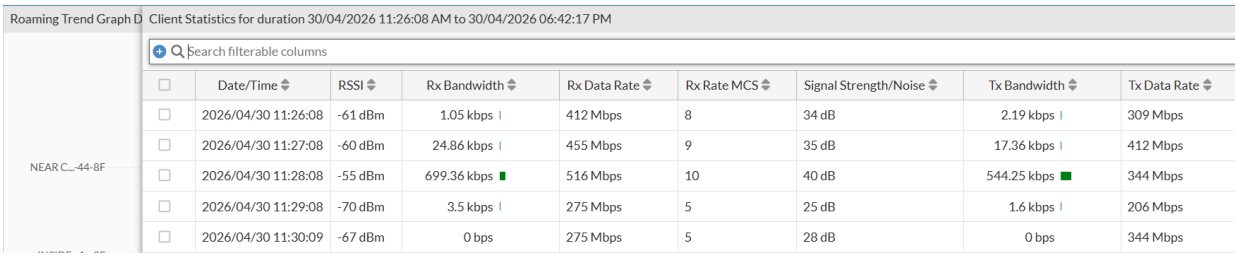
Category	Status / Type	Description
Roaming Status	New Connection	The client successfully completed a full connection to an access point. All phases passed and no SLA breach occurred during the connection process.
	New Connection with Breach	The client's connection attempt resulted in one of the following: • Connection succeeded but one or more phases exceeded the configured SLA threshold. • Connection failed at any phase before completion (such as authentication failure or an incomplete connection).
	Roaming	The client successfully roamed from one access point to another using Fast Transition (802.11r) or Standard roam. All roaming phases completed within the configured SLA thresholds.
	Roaming with Breach	The client roam resulted in one of the following: • Client successfully roamed from one access point to another using Fast Transition (802.11r) or Standard Roam, but one or more phases of the roam exceeded the configured SLA threshold. • Roam failed at any phase before completion (such as incomplete roaming).

Category	Status / Type	Description
	Disconnected	The client was disconnected from the access point after a successful stable session.
Roaming Types	Fast Roam	The client roamed between access points using Fast Transition (802.11r). No active call was in progress at the time of the roam.
	Fast Roam with Active Call	The client roamed between access points using Fast Transition (802.11r) while an active voice or video call was in progress.
	Standard Roam	The client roamed between access points using legacy reassociation (without 802.11r). No active call was in progress.
	Standard Roam with Active Call	The client roamed between access points using legacy reassociation while an active voice or video call was in progress.
Transient Association	FT Transient	A transient association lasting less than 5 minutes that includes at least one Fast Transition (802.11r) roaming event. The association may also contain new connections, disconnections, and other events that occurred in the selected time range.
	Non-FT Transient	A transient association lasting less than 5 minutes that does not include a Fast Transition (802.11r) roaming event. The association may also contain new connections, standard roaming events, disconnections, or any combination of these in the selected time range.
Other Indicators	SLA Issues	SLA breaches occurred during an active connection between access points. Click the SLA Issues indicator to open the **SLA Breaches** pane displaying SLA Summary and Remediation details.

The timeline is color-coded based on the **Received Signal Strength Indicator (RSSI)**, ranging from red (-90 dBm) indicating poor signal to green (-30 dBm) indicating excellent signal.

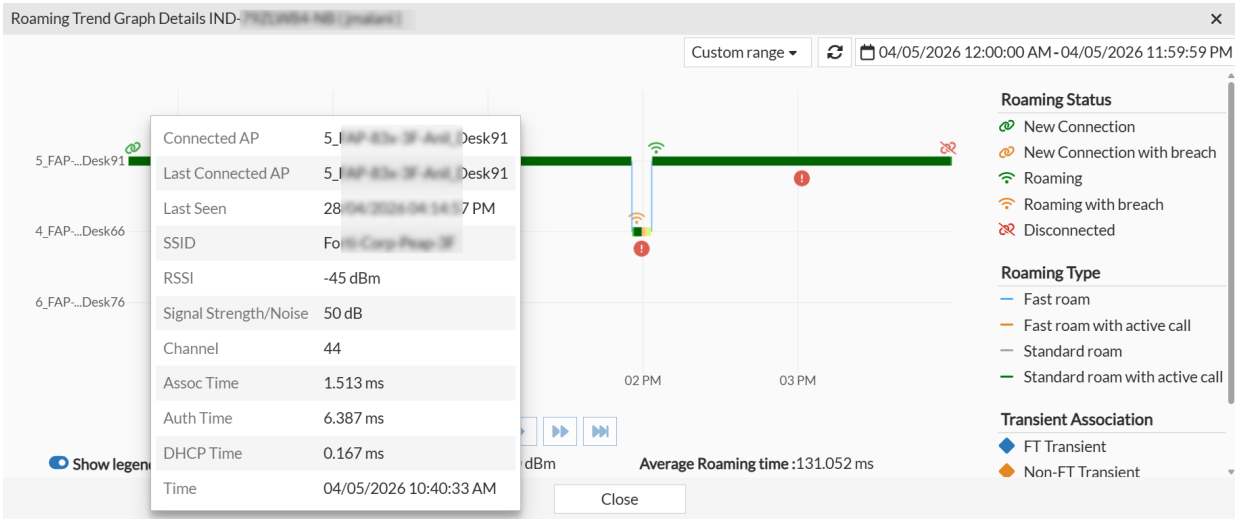
Hovering your cursor over any point on the graph reveals granular, client specific roaming metrics for that moment.

Clicking on the RSSI bar takes you to the **Client Statistics** pane with details such as **RSSI** information, **Rx Bandwidth**, **Rx Data Rate**, **Rx Rate MCS**, **Signal Strength/Noise**, **Tx bandwidth**, **Tx Data Rate**, **Tx Rate MCS**.

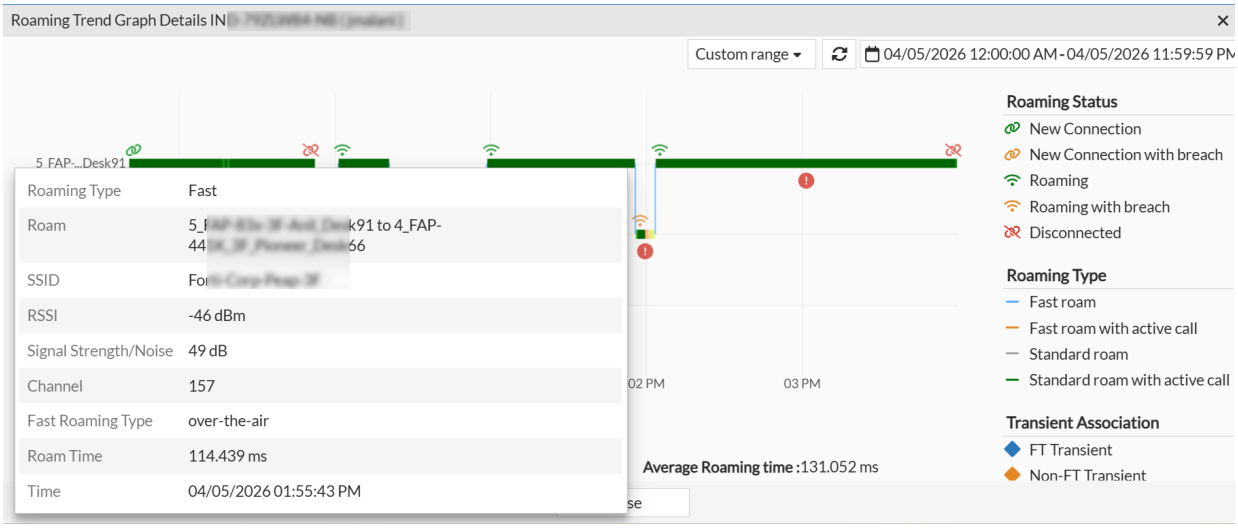


The screenshots below provide examples of these detailed data captures:

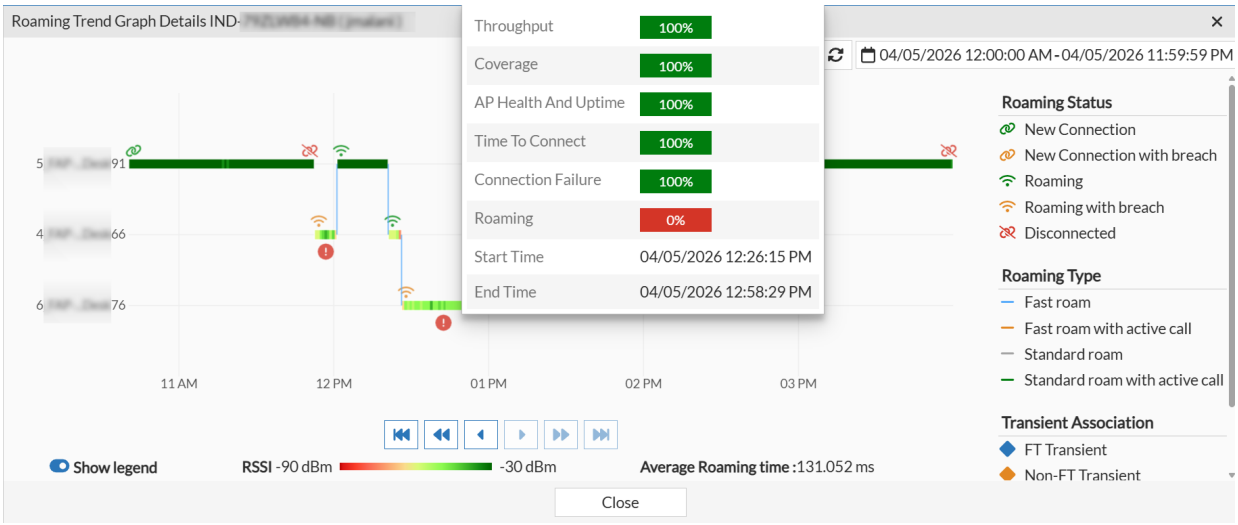
Roaming Status:



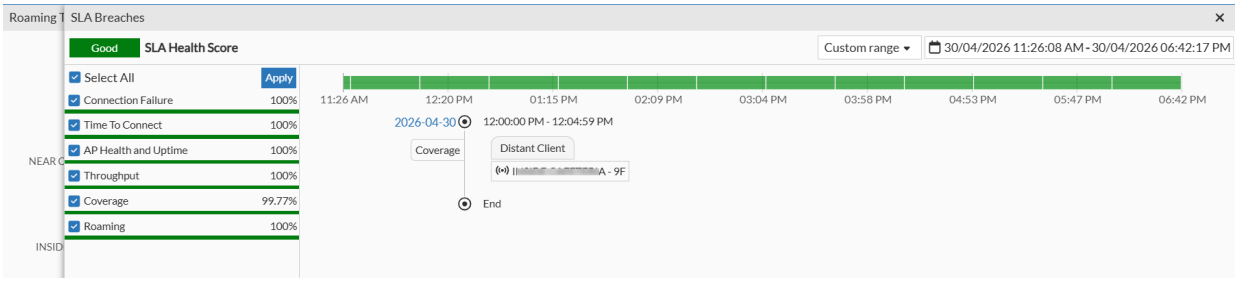
Roaming Type:



SLA Issues:



Clicking on an SLA Issues indicator takes you to SLA Breaches window displaying SLA Summary and Remediation details.



Transient Association:

Clicking on the **Transient Association** icon displays the roaming details of clients within the transient duration.

FortiAIOps 2000G Hardware Support

This release of FortiAIOps supports the FortiAIOps 2000G (FAO-2000G) hardware platform. FAO-2000G comes with FortiAIOps pre-installed.

- By default, the hardware does not include any subscription or device support. These services must be purchased separately. For more information, see the *FortiAIOps Ordering Guide.*
- Official FortiAIOps firmware images installed on hardware platforms are signed by the Fortinet Certificate Authority (CA). If an installed image lacks this CA signature, a warning message is displayed on the GUI.

Initial Configuration

After setting up and mounting the appliance on the rack, connect to the FortiAIOps 2000G CLI using the console port and perform the following steps. See, *FortiAIOps 2000G Quick Start Guide*.

1. On the console, login as an admin user with the username `admin`. Do not enter a password.
   You will be prompted to configure a new password after the initial login.
2. Verify the dynamically assigned IP address using the command: `get system interface`
3. Configure a static IP address (recommended) using the command: `config system interface`

Accessing the GUI

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

1. Open a web browser and enter the following URL.
   `https://<fortiaiops_server_IP>`
   Replace `<fortiaiops_server_IP>` with the static IP address you configured.
2. Log in with the username as `admin`.
   - If you already set a password using the CLI, enter it here.
   - If this is your first time logging in, leave the password blank. You will be prompted to configure a new password.

Note: The administrator password is automatically synchronized between the CLI and the GUI.

Supported Devices

The following are the maximum devices supported in FortiAIOps 2000G hardware.

Maximum device count	Supported Mode
• FortiGates - 5000 • FortiSwitches - 15000	AI Insights and Monitoring

Maximum device count	Supported Mode
• FortiExtenders - 5000 • FortiAPs - 30000 • Clients - 100000	

FortiAIOps supports RAID levels 0, 1, 5, and 10. The default configuration uses RAID 50 for HDDs and RAID 5 for SSDs. The following are the storage capacities for RAID levels in the default and maximum FortiAIOps 2000G hardware configurations.

RAID Level	FortiAIOps 2000G Hardware Configuration Default (8 HDDs, 4 SSDs)
Default RAID (HDD - 50, SSD - 5)	108 TB
RAID 0	144 TB
RAID 1	72 TB
RAID 5	123 TB
RAID 10	72 TB

Note:

- For a fresh configuration, completely erase all existing configurations from the hard disks. A factory reset is recommended to ensure all configurations are removed.
- Back up your configuration data before RAID rebuild and migration operations, as these processes are susceptible to errors.
- The 25 Gbps port does not support 1 Gbps data speeds.
- RAID rebuild and migration operations cannot be performed concurrently. However, simultaneous rebuild operations are supported for SSDs and HDDs.
- The system supports the failure of only one HDD and one SSD at a time. Simultaneous failures of multiple HDDs or SSDs may lead to data loss.

Fabric Connectors: FortiManager Deployment Mode

FortiManager is now supported as a **Deployment Mode** via the Fabric Connector.

Instead of communicating with individual devices, FortiAIOps now interfaces directly with FortiManager, ensuring continuous synchronization of network settings. This integration embeds FortiAIOps analytics within the FortiManager dashboard, where clicking any widget provides a transition to the FortiAIOps GUI for deeper analysis.

Additionally, any configuration updates pushed from FortiAIOps to FortiGates (such as AI-ARRP channel changes or client quarantine statuses) are instantly synced back to FortiManager.

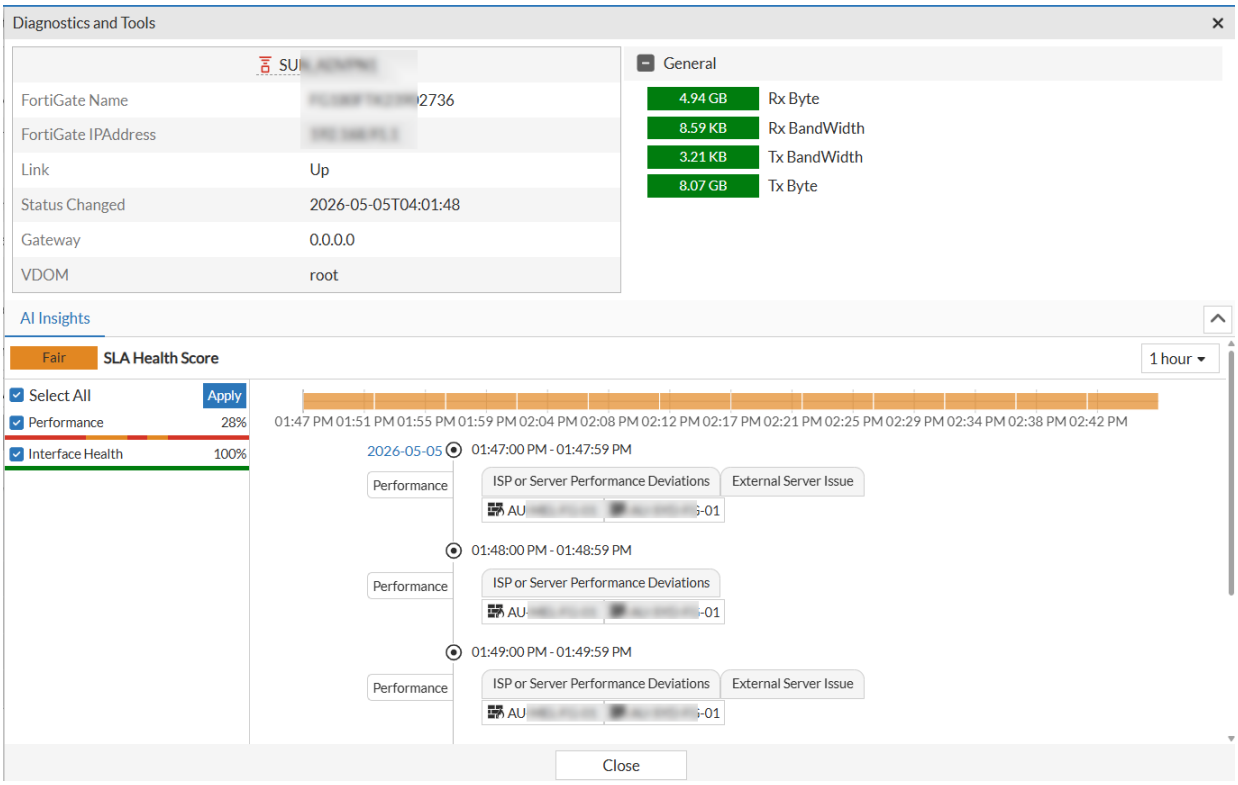
For configuration details, see the *FortiAIOps User Guide for release 3.4*.

SD-WAN Interface Monitoring and AI Insights

This release introduces comprehensive monitoring for SD-WAN interfaces, featuring a new **SD-WAN Interface** tab and advanced **AI Insights** to help administrators analyze performance metrics, identify issues, and determine the root cause of network problems.

Navigate to **Inventory** > **Managed FortiGates**. Select a FortiGate HostName and click **View Details**. Click the **SD-WAN Interfaces** tab.

This tab displays the list of the SD-WAN interfaces available in the FortiGate. To view the details, select a SD-WAN interface and click **View Details**. The **Diagnostics and Tools** pane is displayed.



AI Insights

The **AI Insights** tab helps to analyze various performance metrics, identify issues, and provide detailed insights into the root cause of network problems, helping administrators maintain high service levels.

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:

- Performance
- Interface health

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

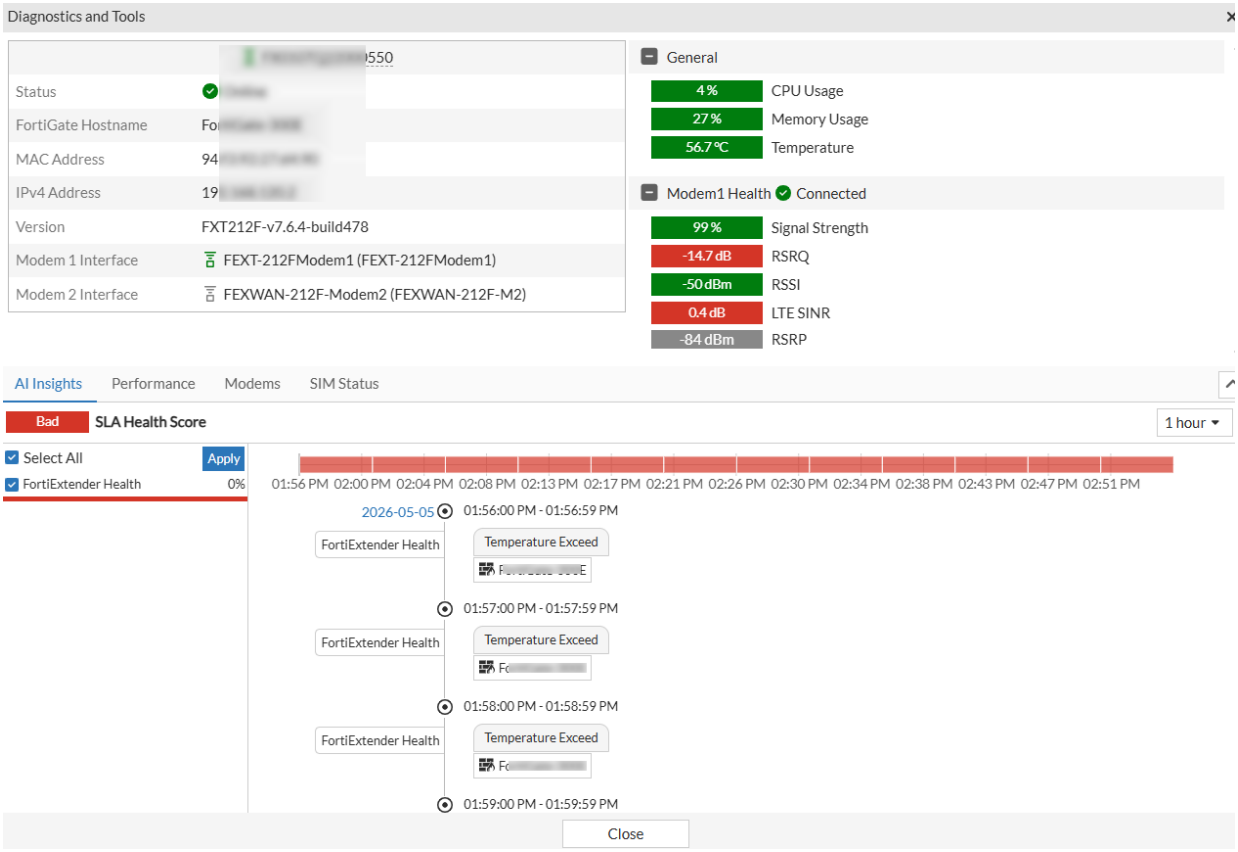
The bar graph shows the performance trend over a selected time period (in this case, 1 day). The graph is divided to equal time segments. Based on the health score of each segment, the segments are color coded as green (good), orange (fair), and red (bad).

Clicking on a specific time segment displays more details events that occurred during the time period.

AI Insights for FortiExtenders

This release introduces a new AI Insights tab within the **Diagnostics and Tools** pane for FortiExtenders. This tab provides the details about the selected Extender and also helps with root-cause analysis and performance tracking to help maintain high service levels.

Navigate to **Extenders** > **FortiExtenders**. Select a FortiExtender and click **View Details**. Click **AI Insights** tab.



Below the overall score, the following metric is available:

- FortiExtender Health

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

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

Clicking on a specific time segment displays more details of the events that occurred during the time period.

Sub-classifier Alarms

Once an acknowledgment is configured, alarms from the following sub-classifiers are now suppressed and automatically marked as **Acknowledged**:

- Client Type
- Asymmetric Data Rates
- Incomplete Connection
- Server Unresponsive and Firewall Policy
- Load Balancing Denied
- Server Unresponsive - Wrong or Missing Cfg Events
- Wrong Credentials
- Capability Mismatch
- No Domain

To ensure metric accuracy, all acknowledged issues are explicitly excluded from network and device health score computations.

Administrators retain the ability to manually edit or delete these alarms. Navigate to **AI Insights** > **Event Acknowledgement** window. Select and acknowledgement from the list to **Edit** or **Delete**.

FortiAI Tokens

FortiAI token allocations map directly to your FortiAIOps license. Your monthly entitled token limit varies depending on the specific license purchased.

Note: Tokens do not stack. If multiple licenses are applied to an account, the license with the highest token limit determines your total allocation.

Token Consumption Hierarchy

- The system prioritizes your Monthly Entitled Tokens first.
- If your monthly entitlement reaches zero before the end of the month, the system uses your Account Tokens (from the Top up license).
- Monthly tokens are only replenished during the scheduled monthly reset.
- If your standard allocation is insufficient, you can purchase FortiAI Assistant token top-up licenses.

For exact allocation details regarding both regular and top-up licenses, refer to the *FortiAIOps Ordering Guide*.

Note: After updating or renewing a license, please allow up to six hours for the system to reflect the new token count.

www.fortinet.com