New Features

FortiLAN Cloud 22.4

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

December 10, 2022
FortiLAN Cloud 22.4 New Features
53-224-859687-20221210

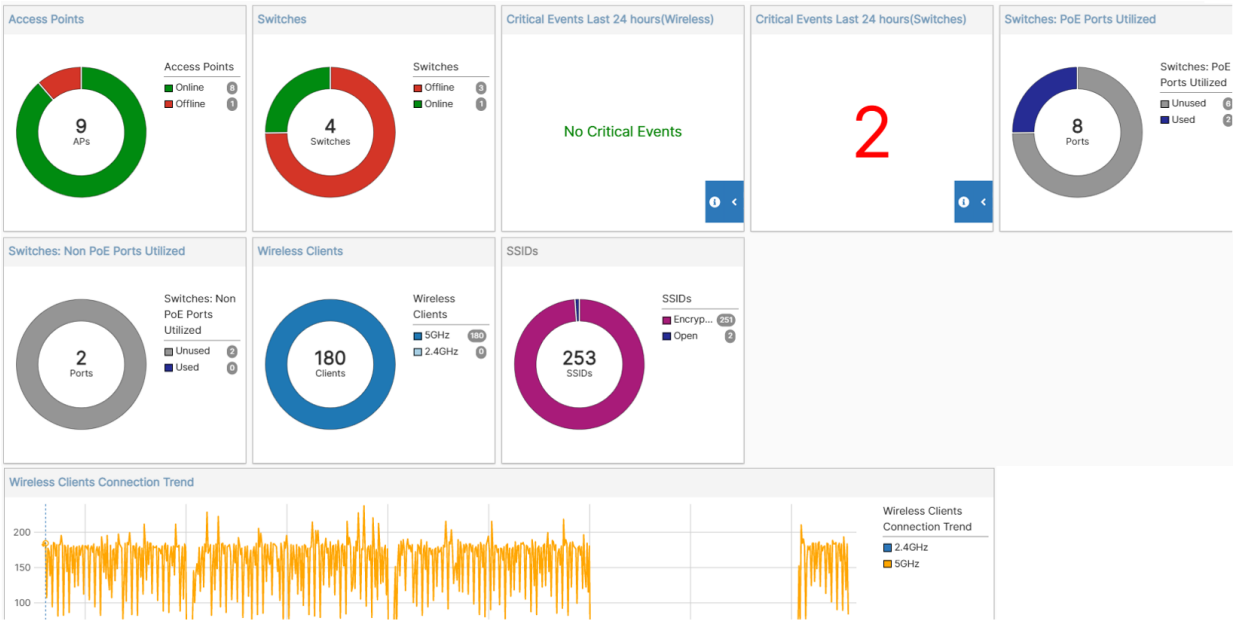
TABLE OF CONTENTS

Change log

Date	Change description
2022-12-10	FortiLAN Cloud 22.4 release document.

FortiLAN Cloud Network Summary Dashboard

The new unified FortiLAN Cloud dashboard combines information from FortiAPs and FortiSwitches to display crucial data required for troubleshooting across both network elements.



Wireless

This section lists the features implemented on the FortiAPs in this release.

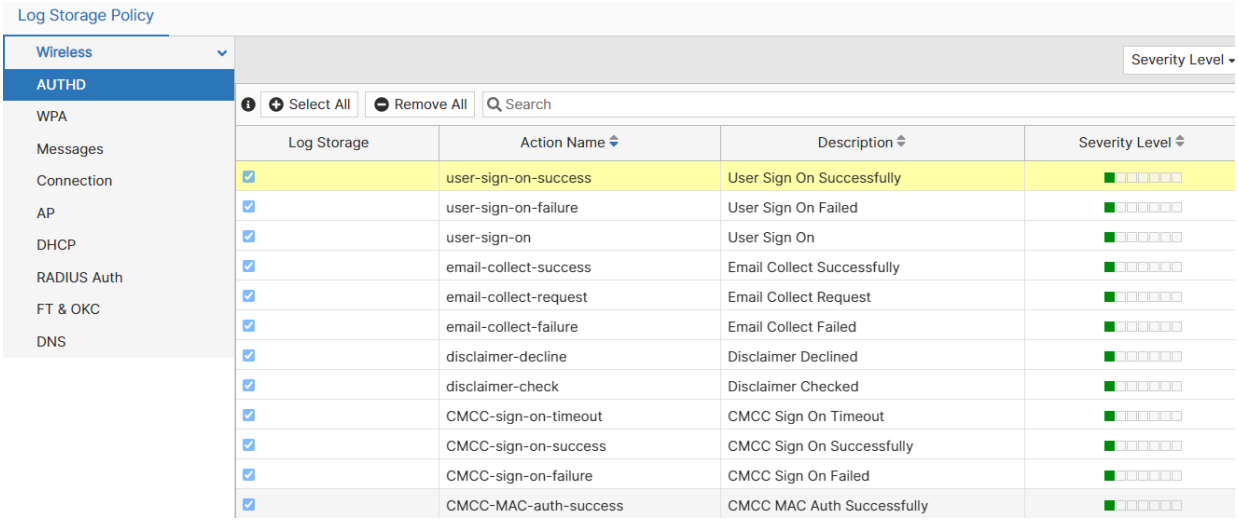
Note: To strengthen security, TLS 1.0 is deprecated as part of this release upgrade. After upgrade, FortiAPs with firmware 6.0.1 or later continue to function but FortiAPs with firmware 5.4 and 5.6 are expected to lose connectivity. Contact *Customer Support*, to install the required patch.

Wireless Log Categorization and Storage Control

FortiLAN Cloud generated wireless logs, instrumental in troubleshooting networks, are stored in the database for 1 year (subscription based). Given that wireless logs can be voluminous depending on the network size, you can now segregate them into multiple different categories and manage the categories to store and display, as per requirement. For example, frame-level logs such as probe logs, authentication logs, and association logs are only required during a debug session and are not always needed. This feature enables you to swiftly filter-down to specific logs of interest.

The network specific log storage policy (settings) configuration overrides the default log storage policy. Navigate to **Wireless > Logs > Settings** to view and manage the log record storage. The log types are displayed on the left panel, select the relevant log type and view the current log storage policy. FortiLAN Cloud assigns each log a severity level.

In the **Log Storage** column, enable/disable the storing of logs and click **Apply**. To reset the log storage policy to the default setting, click **Reset to Defaults** and to reload the saved log storage configuration, click **Reload Saved Config**.



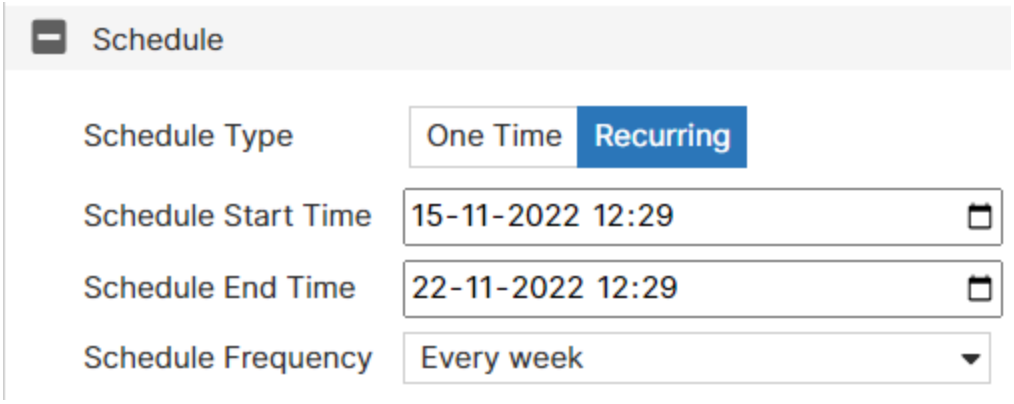
Additional FortiAP Support

FortiLAN Cloud can now additionally manage the following FortiAPs.

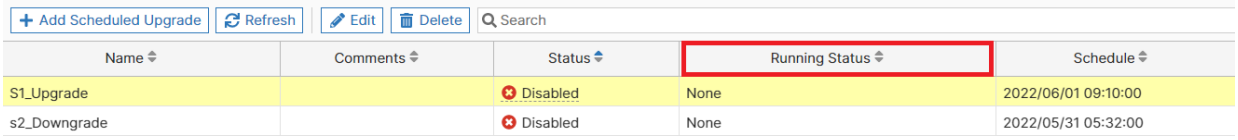
- FortiAP G series models - FAP231G, FAP233G, FAP431G, and FAP433G
  These FortiAPs support WiFi 6E Tri-band and dual 5 GHz modes.
- FortiAP FL series models - FAP231FL, FAP431FL, and FAP433FL

Scheduled Upgrade Enhancements

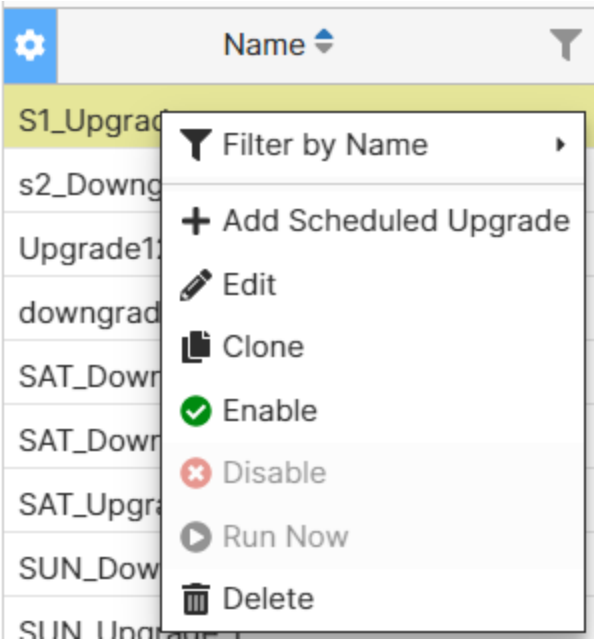
The **Scheduled Upgrade** profiles are enhanced for both Wireless and FortiSwitch to include additional configuration/information. You can now create a recurring schedule in **Configuration > Scheduled Upgrades**.



The Schedule Upgrade page now displays the **Running Status**.



The following management options are added. Select a displayed profile and right-click.



- **Add Scheduled Upgrade** – To create a new Scheduled Upgrade profile.
- **Clone** – You can clone an existing profile with a new name, the cloned profile is disabled (default).
- **Enable/Disable** – You can enable or disable the selected profile(s).
- **Run Now** – This is allowed only for enabled profiles that are not running. If you select multiple profiles, then at least one of them should not be running.
- **Firmware Upgrade Status** - You can view the status of the firmware upgrade for FortiAPs from the edit page.

Wireless Intrusion Detection and Suppression (WIDS)

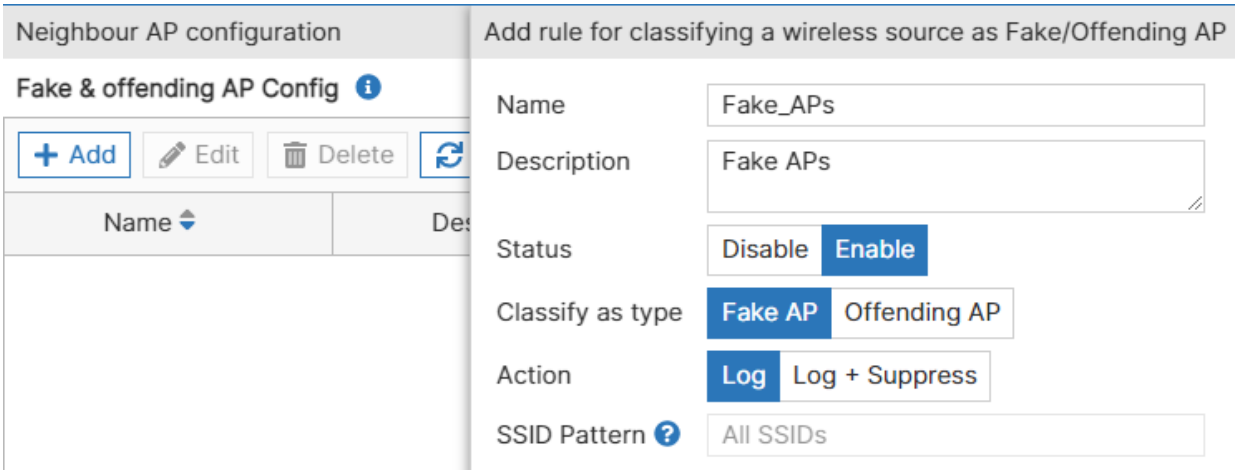
With this release, you can configure rules for automatic detection of fake and offending SSIDs. Additionally, it is also possible to configure actions and counter measures to be taken when these categories of threats are detected. FortiLAN Cloud actively scans and reports the neighbour APs to identify other access points in the area to know their potential impact on the FortiAPs managed by FortiLAN Cloud. You can define the policy to classify the detected neighbour access points **Fake & Offending** and **Rogue & Accepted**. Navigate to **Wireless > Monitor > Neighbour APs**.

Fake & Offending

Fake and Offending categories include phishing access points that lead clients to connect to fake/offending access points instead of getting connected to legitimate FortiAPs. A fake access point broadcasts the same

SSID as the legitimate FortiAP and an offending access point broadcasts SSIDs that falsely represent the company/organization/department of the legitimate FortiAP.

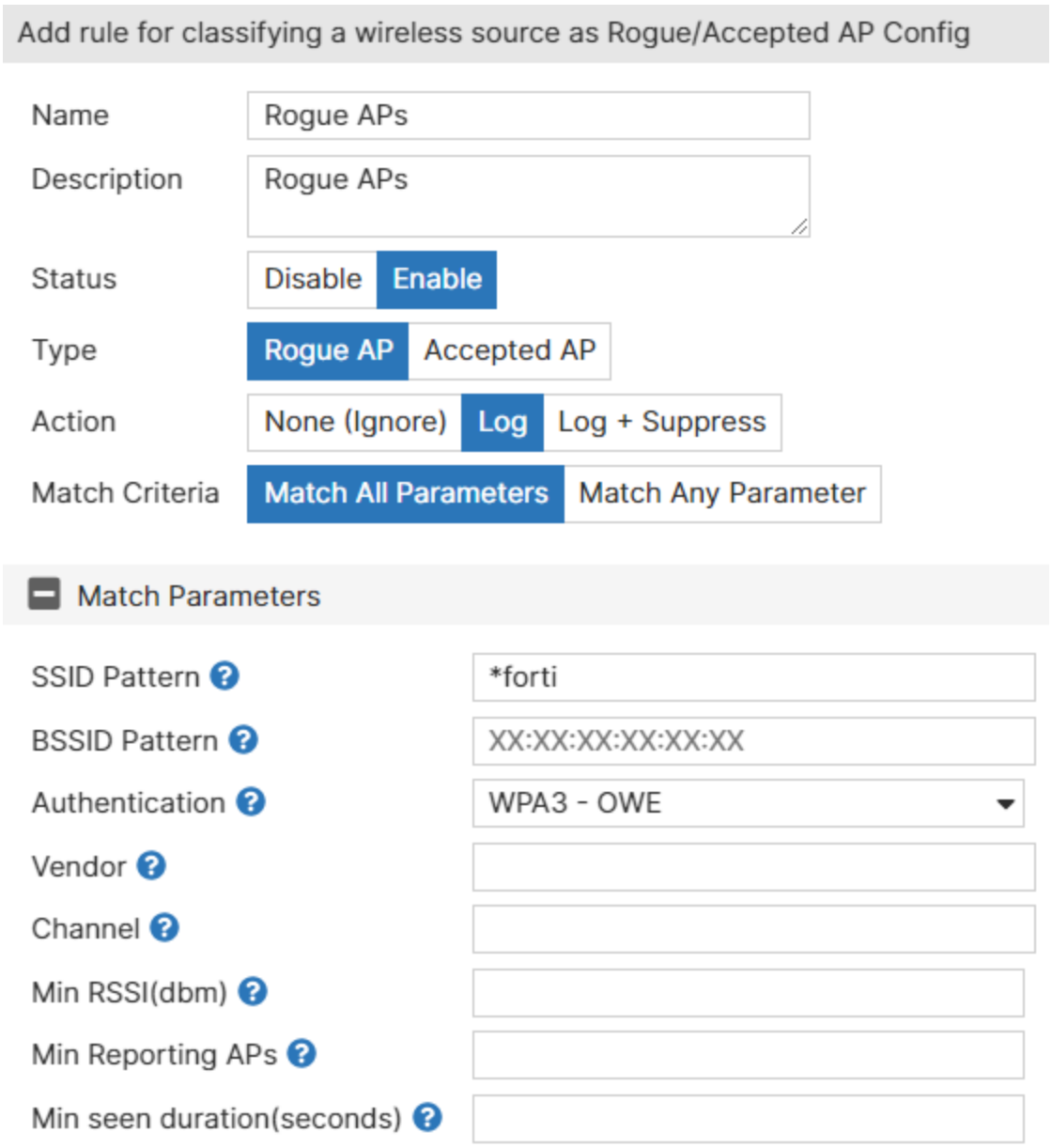
You can configure the criteria for classifying the detected neighbour access points as fake or offending. FortiLAN Cloud compares the received neighbour access point data with the configured policy (SSID) and in case of a match, categorizes them and takes the action as per the configured policy parameters.



Rogue & Accepted

A neighbour access point that could potentially affect the performance of the FortiAPs managed by FortiLAN Cloud, is classified as rogue and a neighbour access point with no adverse impact or interference in the FortiAP wireless network operations are deemed acceptable.

You can configure a single or multiple parameters for the classification of FortiAPs as rogue or acceptable. FortiLAN Cloud compares the received neighbour access point data with the configured parameters and in case of a match, categorizes them and takes the action as per the configured policy parameters.



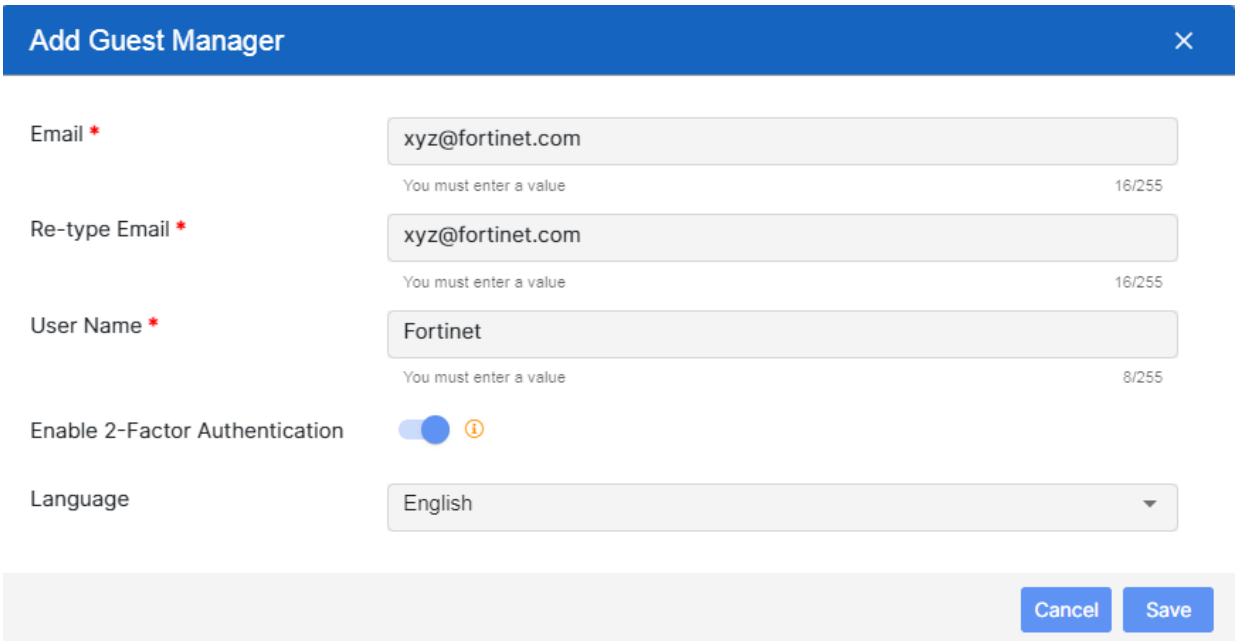
Notes:

- SSID and BSSID patterns allow up to one wildcard (*) character.
- You can create multiple configuration profiles and each configuration profile can specify only a single SSID/BSSID pattern.
- The specified SSID pattern is case-insensitive.

Captive Portal Enhancements

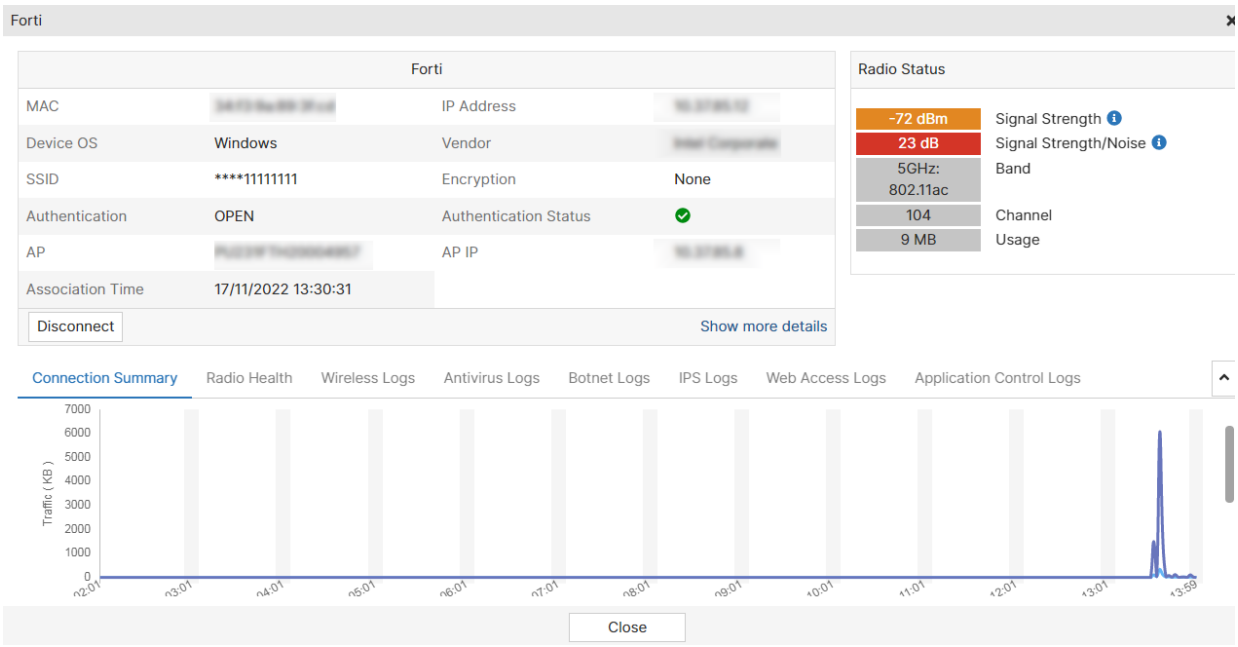
The following options are additionally added in **Wireless > Configuration > FortiLAN Cloud User/Group**.

- Download user data in a *.csv* format for all users/groups,  .
- Import data for **Guest** users,  .
- 2-Factor authentication configuration is added for Email **Guest Manager**.



Wireless Client Dashboard

The wireless client dashboard provides a single pane view with all information and operations related to a connected wireless client, for quick troubleshooting.

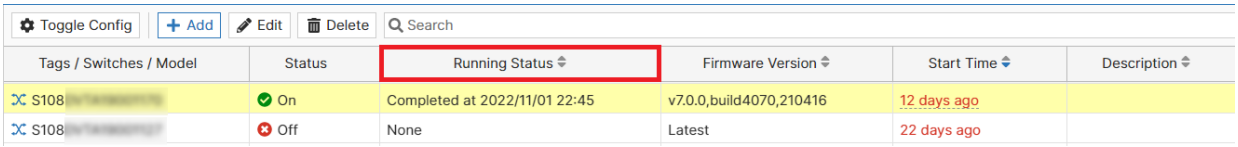

Forti
Forti
MAC
IP Address
Device OS
Windows
Vendor
SSID
****11111111
Encryption
None
Authentication
OPEN
Authentication Status
AP
AP IP
Association Time
17/11/2022 13:30:31
Disconnect
Show more details
Radio Status
-72 dBm
Signal Strength
23 dB
Signal Strength/Noise
5GHz: 802.11ac
Band
104
Channel
9 MB
Usage
Connection Summary
Radio Health
Wireless Logs
Antivirus Logs
Botnet Logs
IPS Logs
Web Access Logs
Application Control Logs
Traffic (KB)
7000
6000
5000
4000
3000
2000
1000
0
Close

FortiSwitch

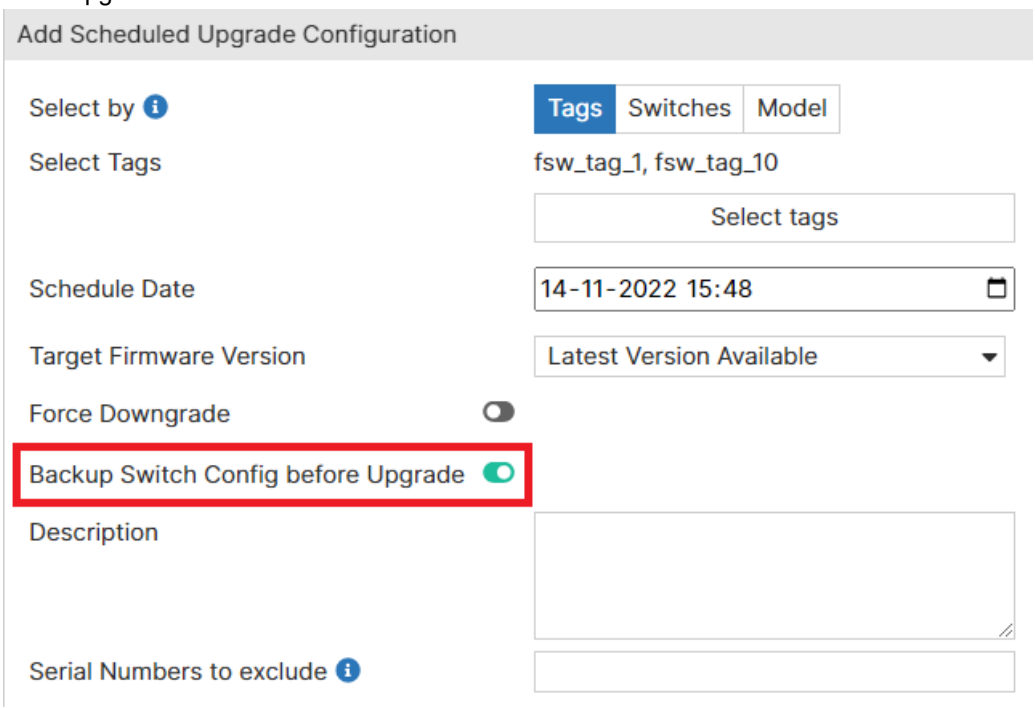
This section lists the features implemented on the FortiSwitches in this release.

Scheduled Upgrade Enhancements

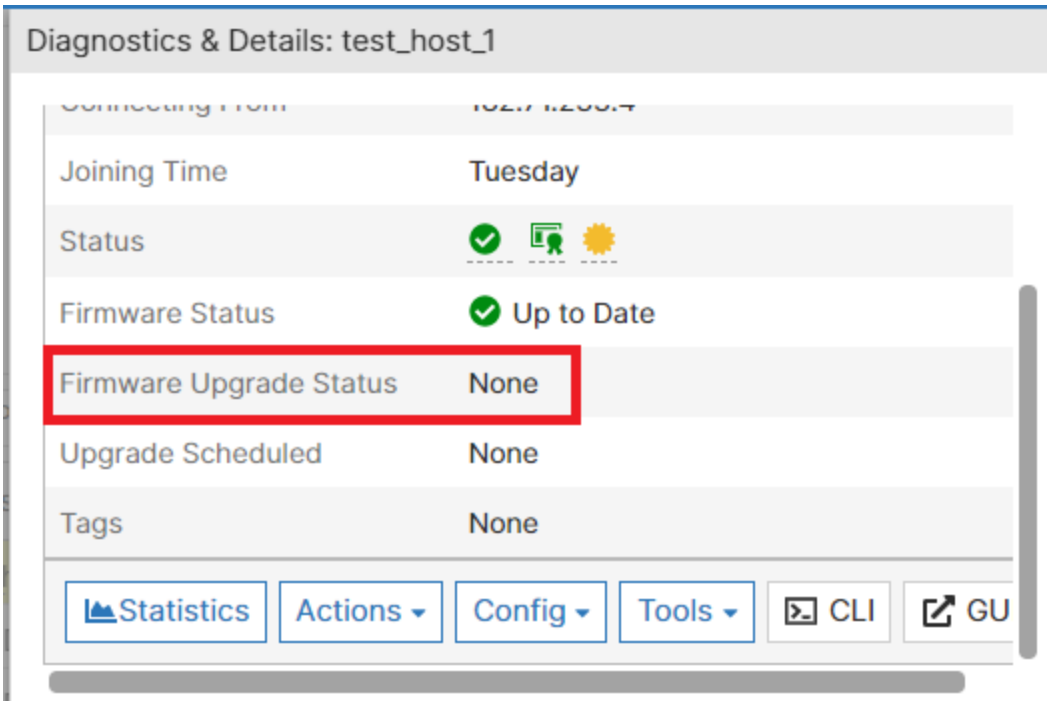
The **Switch > Configuration > Schedule Upgrade** page now displays the **Running Status**.



- **Backup Switch Config before Upgrade** - This enables you to backup the FortiSwitch configuration prior to the upgrade.



- **Firmware Upgrade Status** - You can view the status of the firmware upgrade for all deployed FortiSwitches.



ZTC Enhancements

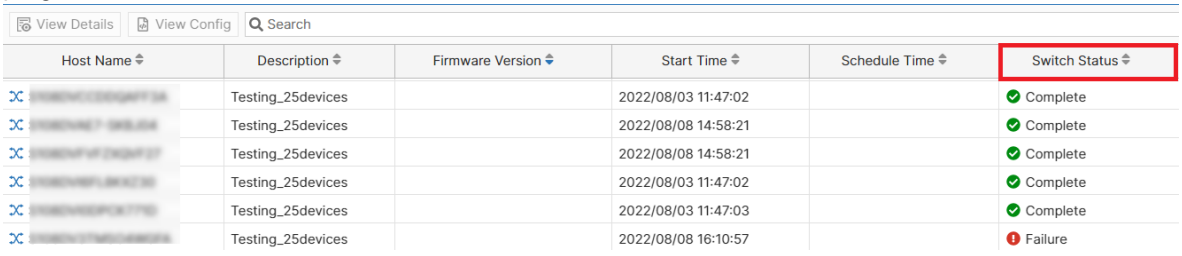
The following ZTC enhancements are delivered in this release.

- ZTC Enhancements
- ZTC Configurations

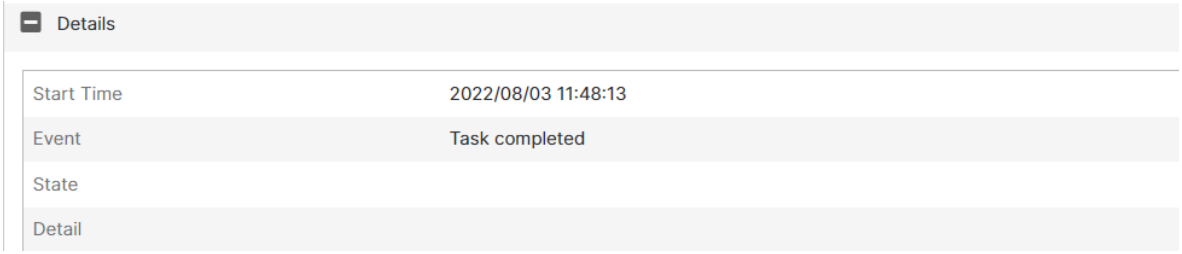
ZTC Feature Progression

You can now view the progression status of the FortiSwitch ZTC application. Navigate to **Switch > Monitor > Zero Touch Config Status** to view the following additional details.

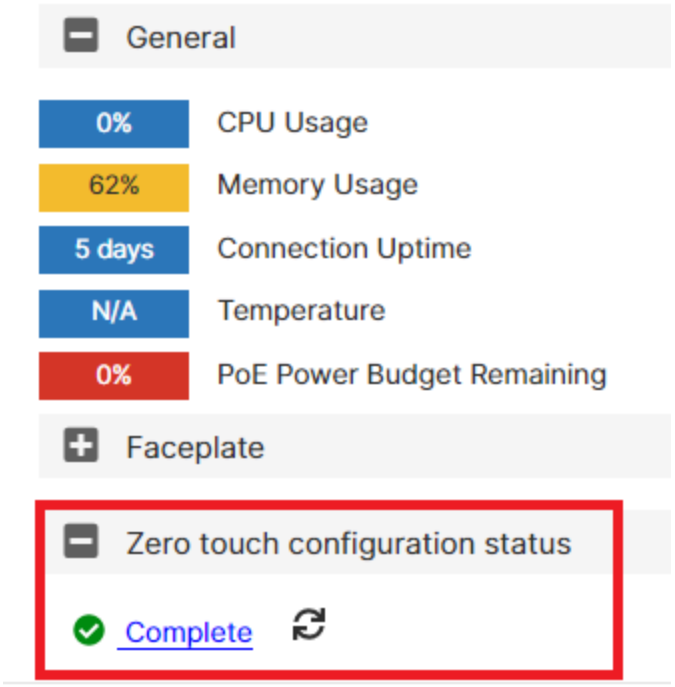
- The **Switch Status** column displays the progress percentage along with the current state the feature progression is in.



- The **View Details** tab displays the update of ongoing/accomplished tasks.

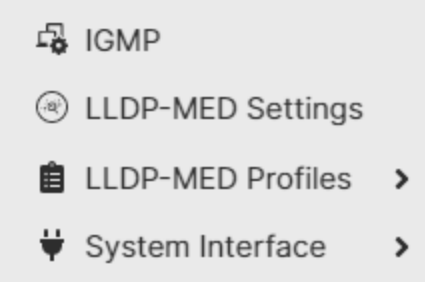


- The **Diagnostics & Details** tab displays the **Zero touch configuration** status that includes the state of the configuration.



ZTC Configurations

The following configuration that are a part of the ZTC templates in FortiLAN Cloud, are now available as separate profiles. You can apply these profiles directly on the FortiSwitch. In these profiles, you can review the current configuration on the FortiSwitch, modify a few selected items, and re-apply the config to the device(s).



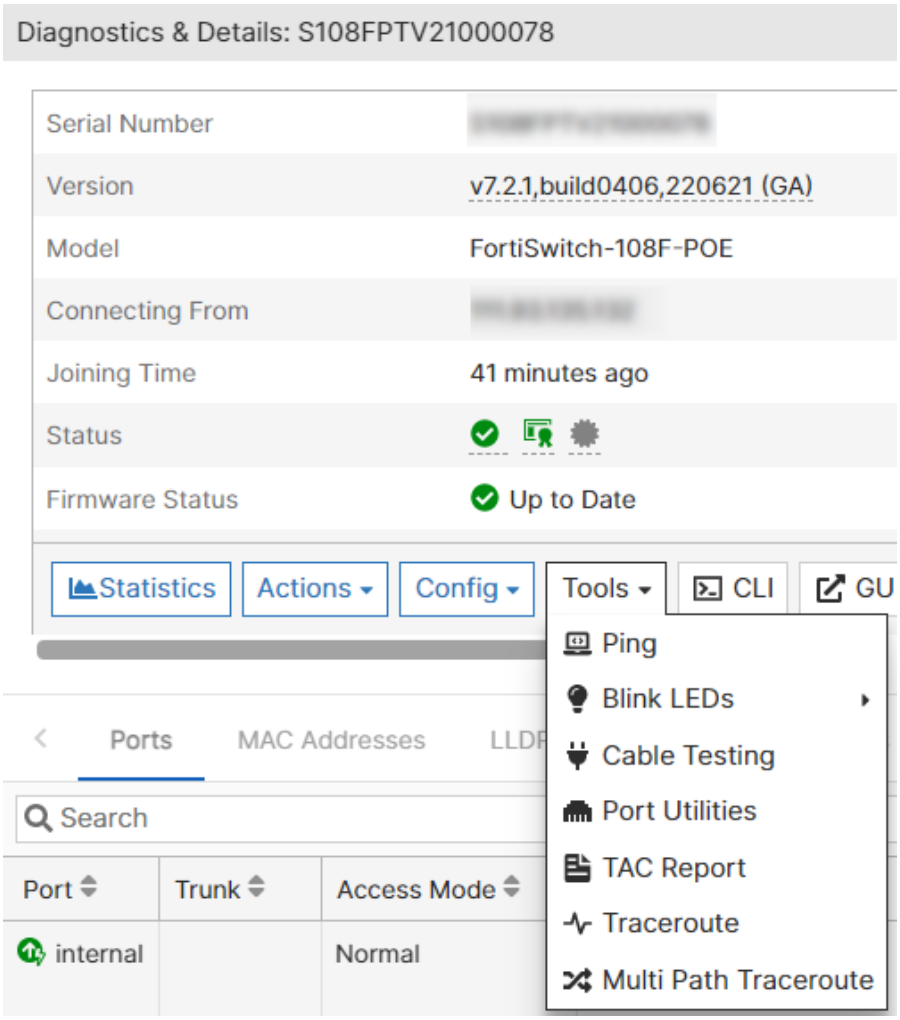
- IGMP
- System VLAN Interface

- System Physical Interface
- LLDP Settings
- LLDP Profiles

Note: A maximum of 255 profiles are supported per network.

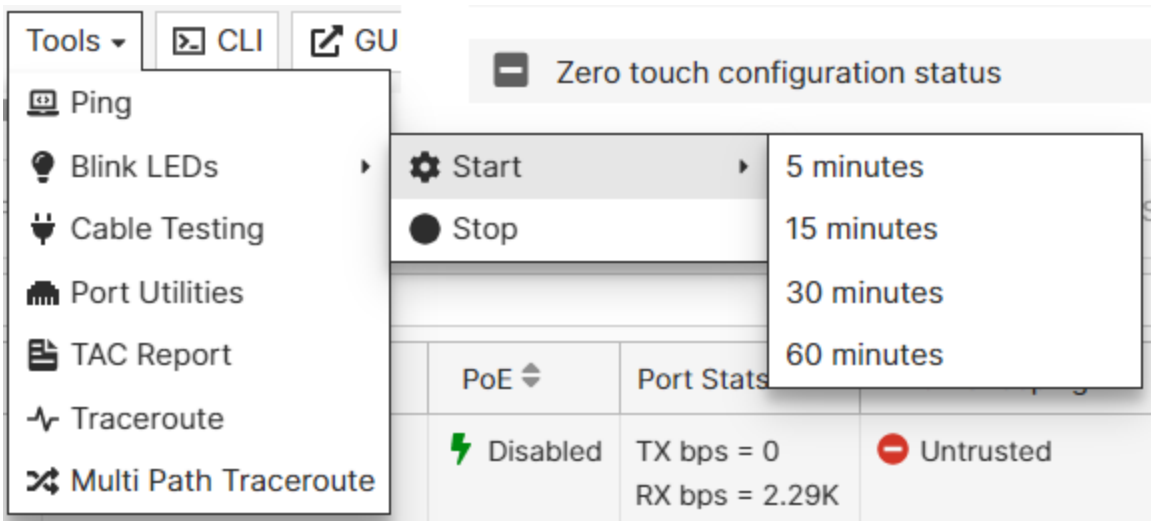
Tools

The following troubleshooting tools are added in FortiSwitch. You can access them from the **Diagnostics and Tools** panel.



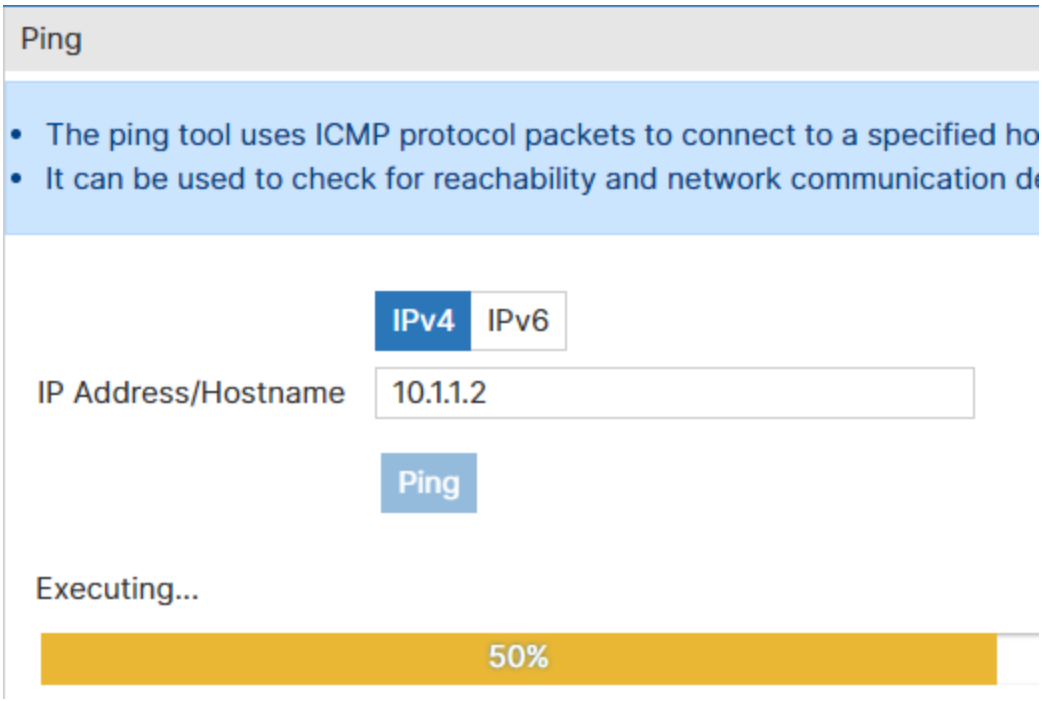
Blink LEDs

Starting this operation, blinks the FortiSwitch LEDs for a specific time period. This is used to identify the physical location of a specific switch/port in a rack. Click **Start** and select a time duration, to stop the blinking LEDs before the configured time, click **Stop**.



Ping

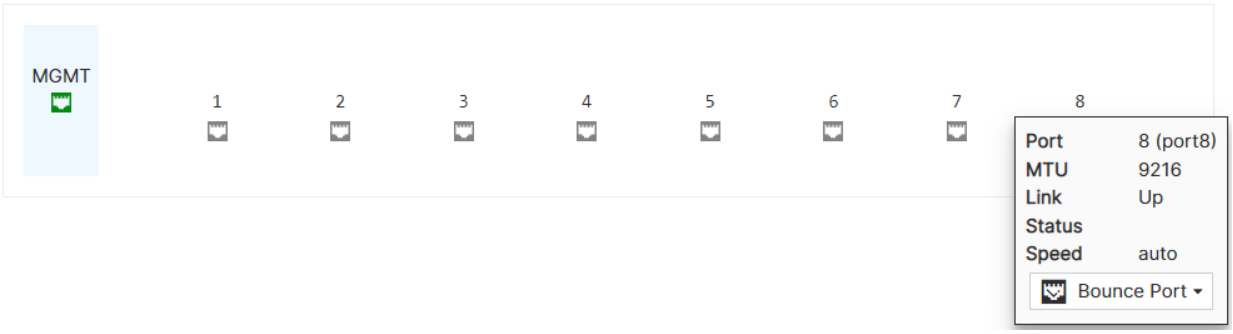
The ping command sends data packets to a specific IP address on a network, and then lets you know how long it took to transmit that data and get a response. This is used to determine reachability of the FortiSwitch to other devices on the internal or external Internet. You can conduct a ping test to an IP/domain from a FortiSwitch for troubleshooting, reachability and other network connectivity issues. The ping tool uses ICMP protocol packets to connect to a specified host. Both IPv4 and IPv6 hosts are supported.



Port Utilities

You can use the **Bounce Port** utility to disable a port for a specific period of time. This allows you to isolate problematic clients or force a network reconfiguration on the connected clients. You can stop the bounce port operation mid-way and the connected clients recover immediately.

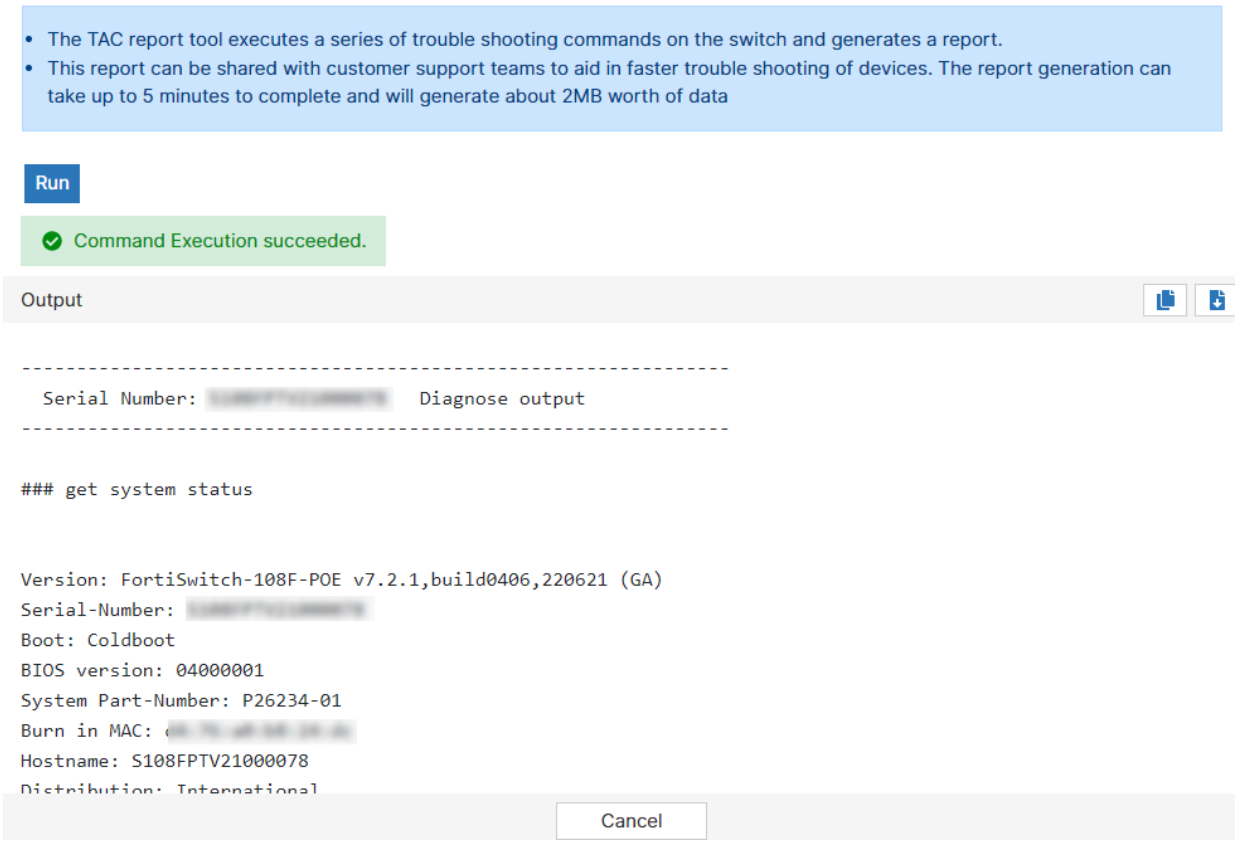
The **PoE Reset** utility resets the power supplied over Ethernet on a specific port. This enables you to reset PoE devices connected to the port, when the devices are located in an environment where physical access is not easily achievable.



TAC Report

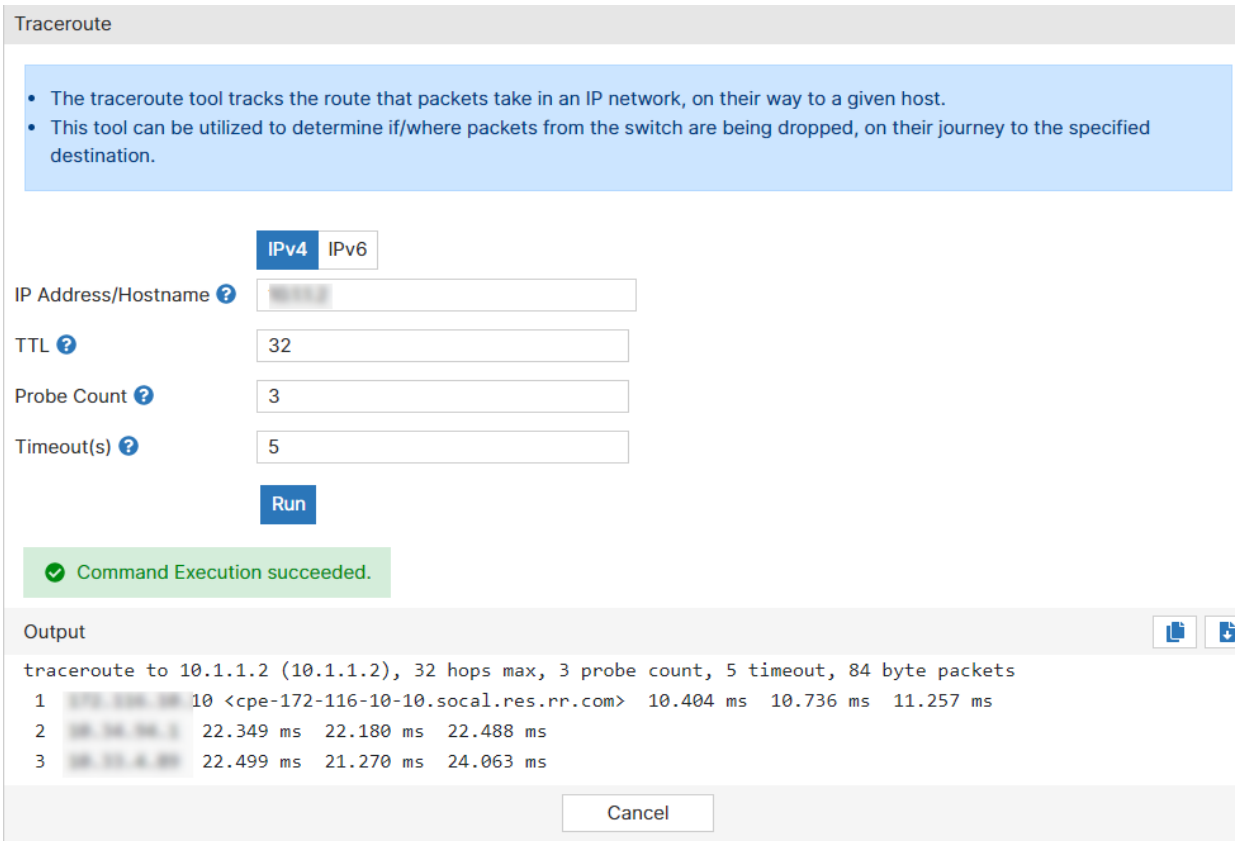
The Technical Assistance Center (TAC) report runs an exhaustive series of diagnostic commands. This report contains a significant amount of information which can be used by the TAC team to analyze issues that a customer is seeing on his FortiSwitch device.

Click **Run**. The report generation can take up to 5 minutes to complete and generates approximately 2 MB worth of data.



Traceroute

The traceroute tool utilizes ICMP packets to trace the different servers/routers that a packet visits, on its journey to a specified host. This tool is used to determine specific points in a network with bottle necks/traffic drops.



Update the following configuration for IPv4.

- **IP Address/Hostname** – The IPv4 address or host name to trace the route to.
- **TTL** – The maximum time-to-live (number of hops) that the route can take. The valid range is 1 – 64 and the default is 32.
- **Probe Count** – The number of probes to use to trace the route. The valid range is 1 – 5 and the default is 3.
- **Timeout(s)** – The time duration that the route is probed for, before the trace route stops. The valid range is 1 – 10 seconds and the default is 5 seconds.

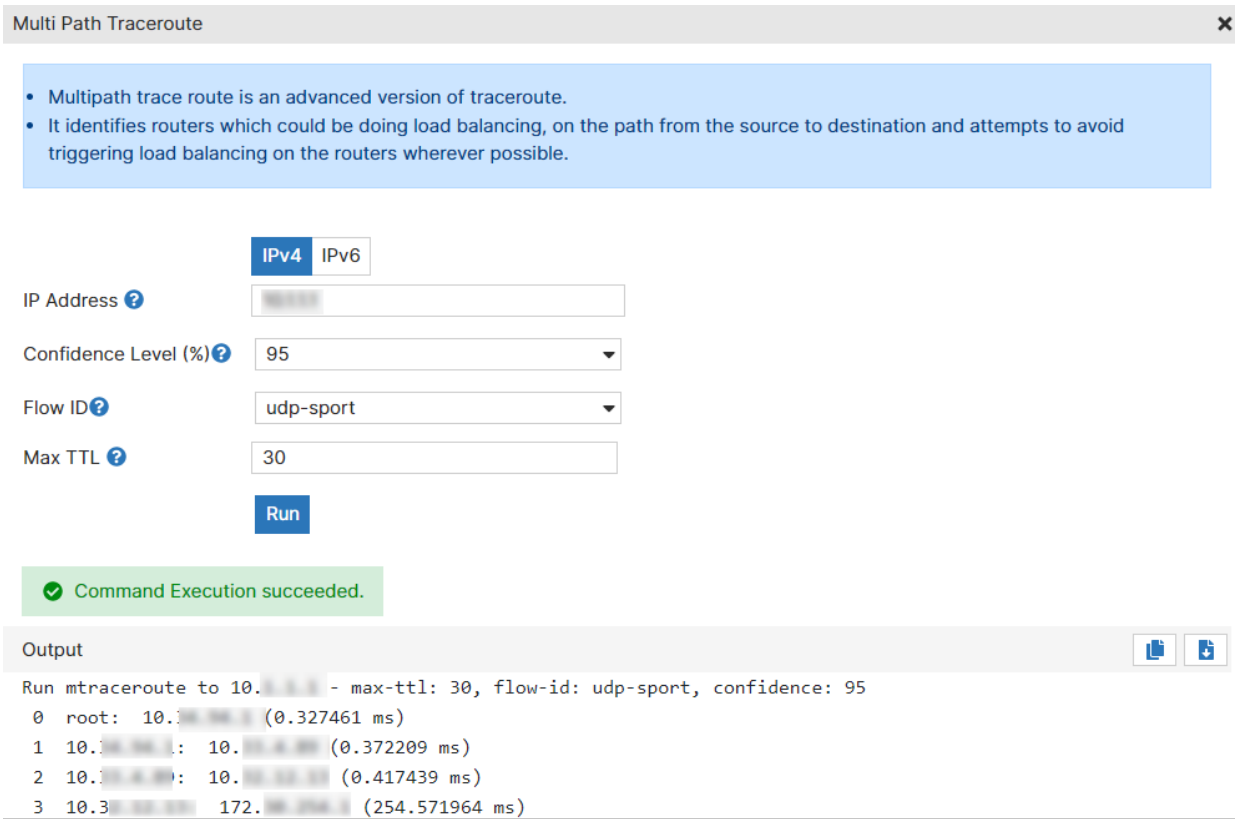
Update the following configuration for IPv6.

- **IP Address/Hostname** – The IPv6 address or host name to trace the route to.
- **Fragment** – Enable/disable the Don't Fragment flag.
- **Resolve Name** – Enable resolving the numeric address to domain name.
- **Max TTL** – The maximum number of hops used in outgoing probe packets. The valid range is 1 – 255 and the default is 30.

Multi Path Traceroute

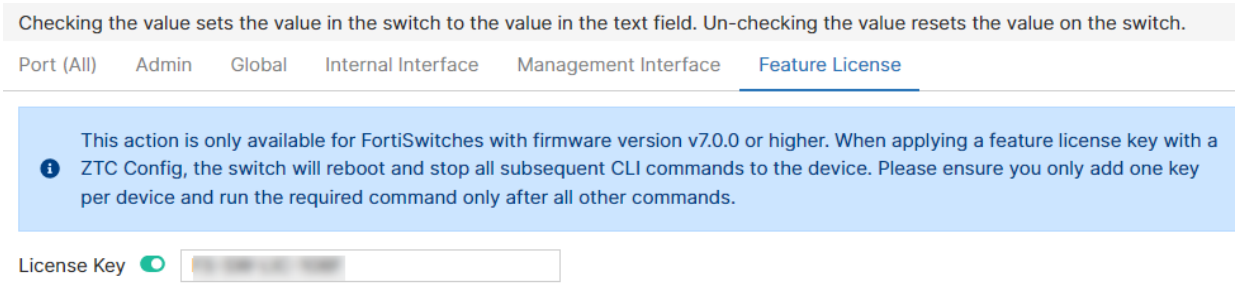
This is an advanced version of traceroute that identifies routers which could be load balancing on the path from the source to destination. It attempts to avoid triggering load balancing on the routers, wherever possible. Update the following configuration for IPv4/IPv6.

- **IP Address** - The IP address or host name to trace the route to.
- **Confidence Level (%)** – Select the confidence level. The allowed values are 90, 95, and 99, the default is 95.
- **Flow ID** – Select the flow identifier.
- **Max TTL** - The maximum time-to-live (number of hops) used in outgoing probe packets. The valid range is 1 – 255 and the default is 30.



Feature License

You can now add and remove the FortiSwitch feature license from the FortiLAN Cloud GUI. This operation is supported in the **Basic Configuration** and **Actions** panel of deployed FortiSwitches.



Note: The feature license management option is supported only on firmware version 7.0 and above.

www.fortinet.com