

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

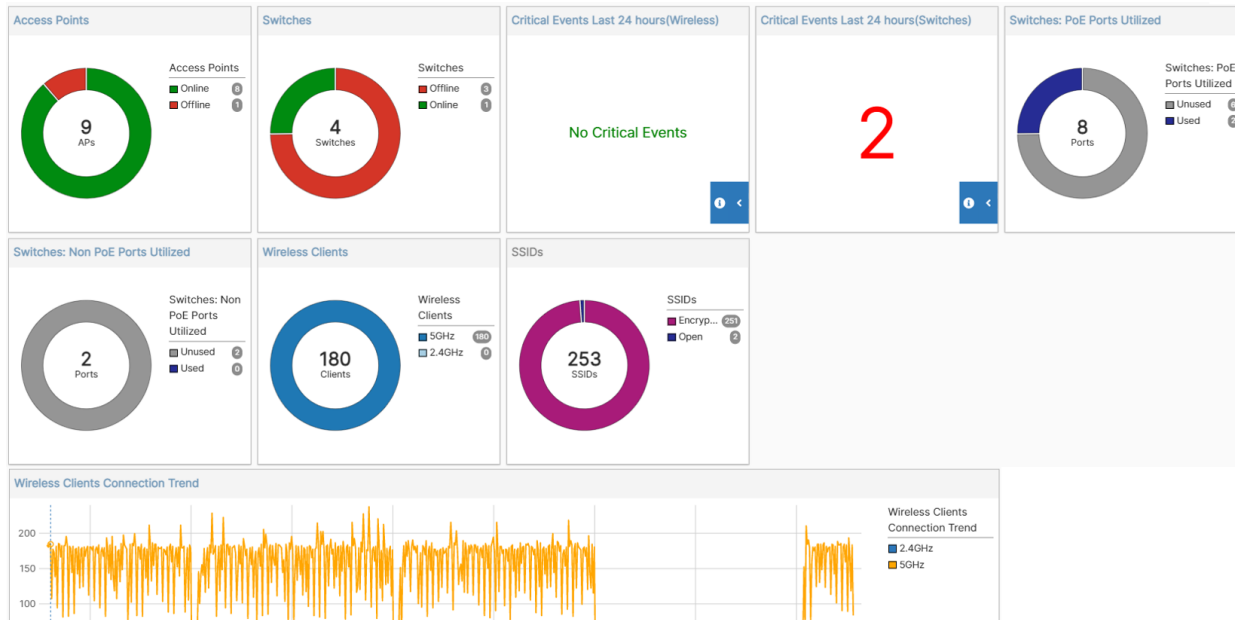
Change log	4
FortiLAN Cloud Network Summary Dashboard	5
Wireless	6
Wireless Log Categorization and Storage Control	6
Additional FortiAP Support	7
Scheduled Upgrade Enhancements	7
Wireless Intrusion Detection and Suppression (WIDS)	8
Captive Portal Enhancements	10
Wireless Client Dashboard	11
FortiSwitch	13
Scheduled Upgrade Enhancements	13
ZTC Enhancements	14
Tools	16
Blink LEDs	16
Ping	17
Port Utilities	18
TAC Report	18
Traceroute	19
Multi Path Traceroute	20
Feature License	21

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.

- [Wireless Log Categorization and Storage Control](#)
- [Additional FortiAP Support](#)
- [Scheduled Upgrade Enhancements](#)
- [Wireless Intrusion Detection and Suppression \(WIDS\)](#)
- [Captive Portal Enhancements](#)
- [Wireless Client Dashboard](#)

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**.

Log Storage Policy

Wireless

AUTHD

WPA

Messages

Connection

AP

DHCP

RADIUS Auth

FT & OKC

DNS

Severity Level

Select All Remove All Search

Log Storage	Action Name	Description	Severity Level
<input checked="" type="checkbox"/>	user-sign-on-success	User Sign On Successfully	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	user-sign-on-failure	User Sign On Failed	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	user-sign-on	User Sign On	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	email-collect-success	Email Collect Successfully	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	email-collect-request	Email Collect Request	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	email-collect-failure	Email Collect Failed	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	disclaimer-decline	Disclaimer Declined	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	disclaimer-check	Disclaimer Checked	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	CMCC-sign-on-timeout	CMCC Sign On Timeout	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	CMCC-sign-on-success	CMCC Sign On Successfully	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	CMCC-sign-on-failure	CMCC Sign On Failed	■ □ □ □ □ □ □ □
<input checked="" type="checkbox"/>	CMCC-MAC-auth-success	CMCC MAC Auth Successfully	■ □ □ □ □ □ □ □

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**.

[-] Schedule

Schedule Type One Time Recurring

Schedule Start Time

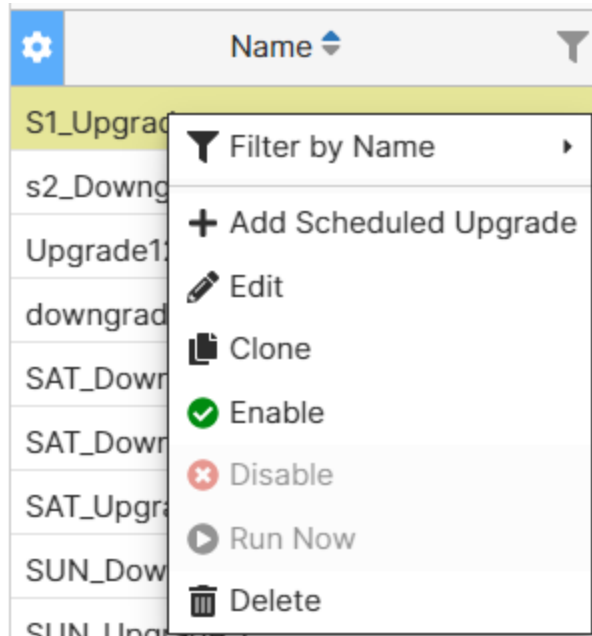
Schedule End Time

Schedule Frequency

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

Name	Comments	Status	Running Status	Schedule
S1_Upgrade		Disabled	None	2022/06/01 09:10:00
s2_Downgrade		Disabled	None	2022/05/31 05:32:00

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.

Neighbour AP configuration
Add rule for classifying a wireless source as Fake/Offending AP

Fake & offending AP Config i

+ Add
✎ Edit
🗑 Delete
↻

Name	Description

Name	<input type="text" value="Fake_APs"/>
Description	<input style="height: 30px;" type="text" value="Fake APs"/>
Status	Disable Enable
Classify as type	Fake AP Offending AP
Action	Log Log + Suppress
SSID Pattern ?	<input type="text" value="All SSIDs"/>

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.

Add rule for classifying a wireless source as Rogue/Accepted AP Config

Name	<input type="text" value="Rogue APs"/>
Description	<input type="text" value="Rogue APs"/>
Status	<input type="button" value="Disable"/> <input checked="" type="button" value="Enable"/>
Type	<input checked="" type="button" value="Rogue AP"/> <input type="button" value="Accepted AP"/>
Action	<input type="button" value="None (Ignore)"/> <input checked="" type="button" value="Log"/> <input type="button" value="Log + Suppress"/>
Match Criteria	<input checked="" type="button" value="Match All Parameters"/> <input type="button" value="Match Any Parameter"/>

Match Parameters



SSID Pattern 	<input type="text" value="*forti"/>
BSSID Pattern 	<input type="text" value="XX:XX:XX:XX:XX:XX"/>
Authentication 	<input type="text" value="WPA3 - OWE"/>
Vendor 	<input type="text"/>
Channel 	<input type="text"/>
Min RSSI(dbm) 	<input type="text"/>
Min Reporting APs 	<input type="text"/>
Min seen duration(seconds) 	<input type="text"/>

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**.

Add Guest Manager ✕

Email *
You must enter a value 16/255

Re-type Email *
You must enter a value 16/255

User Name *
You must enter a value 8/255

Enable 2-Factor Authentication ⓘ

Language

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

MAC	[REDACTED]	IP Address	[REDACTED]
Device OS	Windows	Vendor	[REDACTED]
SSID	****11111111	Encryption	None
Authentication	OPEN	Authentication Status	✓
AP	[REDACTED]	AP IP	[REDACTED]
Association Time	17/11/2022 13:30:31		

[Disconnect](#) [Show more details](#)

Radio Status

-72 dBm	Signal Strength
23 dB	Signal Strength/Noise
5GHz:	Band
802.11ac	
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)

Close

FortiSwitch

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

- [Scheduled Upgrade Enhancements](#)
- [ZTC Enhancements](#)
- [Tools](#)
- [Feature License](#)

Scheduled Upgrade Enhancements

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

Tags / Switches / Model	Status	Running Status	Firmware Version	Start Time	Description
S108	On	Completed at 2022/11/01 22:45	v7.0.0,build4070,210416	12 days ago	
S108	Off	None	Latest	22 days ago	

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

Add Scheduled Upgrade Configuration

Select by i Tags Switches Model

Select Tags fsw_tag_1, fsw_tag_10

Select tags

Schedule Date 14-11-2022 15:48 📅

Target Firmware Version Latest Version Available ▼

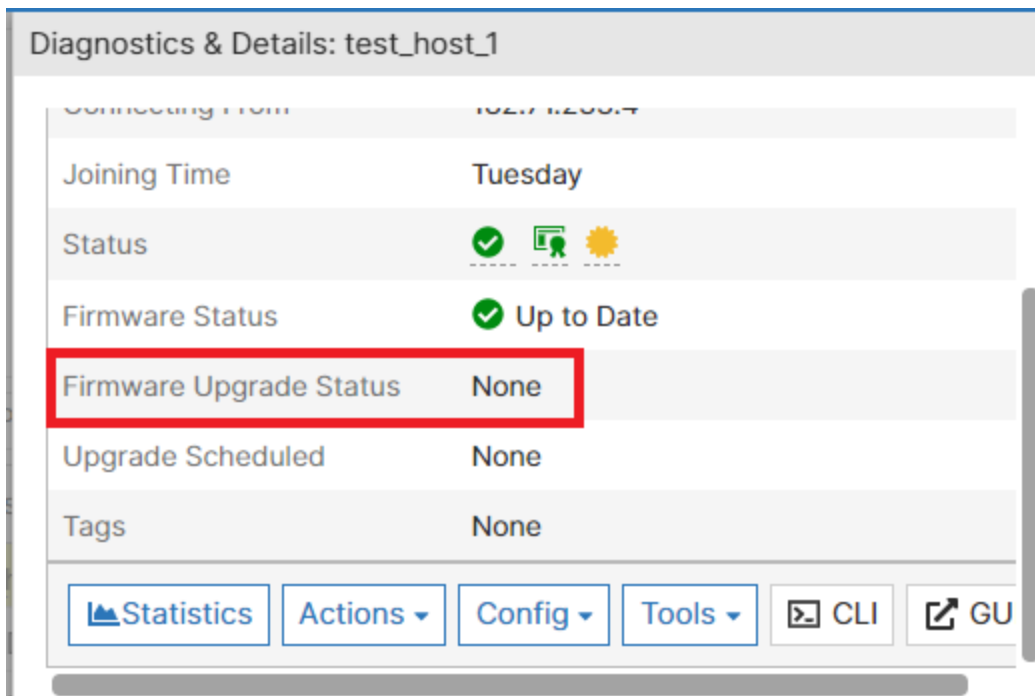
Force Downgrade

Backup Switch Config before Upgrade

Description

Serial Numbers to exclude i

- **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.

Host Name	Description	Firmware Version	Start Time	Schedule Time	Switch Status
Testing_25devices	Testing_25devices		2022/08/03 11:47:02		Complete
Testing_25devices	Testing_25devices		2022/08/08 14:58:21		Complete
Testing_25devices	Testing_25devices		2022/08/08 14:58:21		Complete
Testing_25devices	Testing_25devices		2022/08/03 11:47:02		Complete
Testing_25devices	Testing_25devices		2022/08/03 11:47:03		Complete
Testing_25devices	Testing_25devices		2022/08/08 16:10:57		Failure

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

Details	
Start Time	2022/08/03 11:48:13
Event	Task completed
State	
Detail	

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

- General

0%

CPU Usage

62%

Memory Usage

5 days

Connection Uptime

N/A

Temperature

0%

PoE Power Budget Remaining

+ Faceplate

- Zero touch configuration status

✓
Complete
↻

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
- ⌚ LLDP-MED Settings
- 📄 LLDP-MED Profiles >
- 🔌 System Interface >

- 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.

Diagnostics & Details: S108FPTV21000078

Serial Number	S108FPTV21000078
Version	v7.2.1,build0406,220621 (GA)
Model	FortiSwitch-108F-POE
Connecting From	192.168.1.100
Joining Time	41 minutes ago
Status	✓ 🔌 ⚙️
Firmware Status	✓ Up to Date

[Statistics](#)
[Actions](#)
[Config](#)
[Tools](#)
[CLI](#)
[GU](#)

[Ports](#)
[MAC Addresses](#)
[LLDP](#)

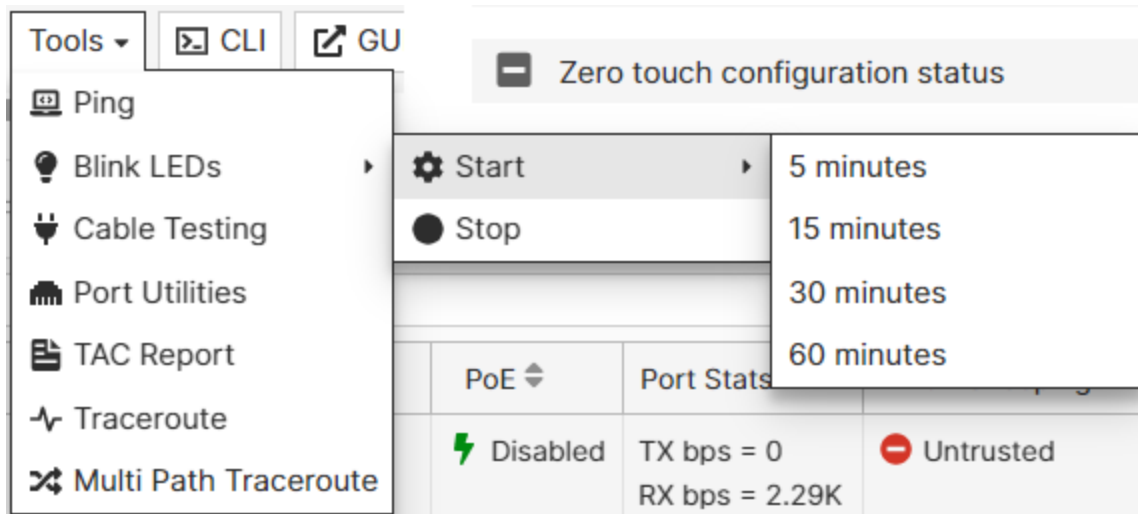
Search

Port	Trunk	Access Mode
🔌 internal		Normal

- Ping
- Blink LEDs
- Cable Testing
- Port Utilities
- TAC Report
- Traceroute
- Multi Path Traceroute

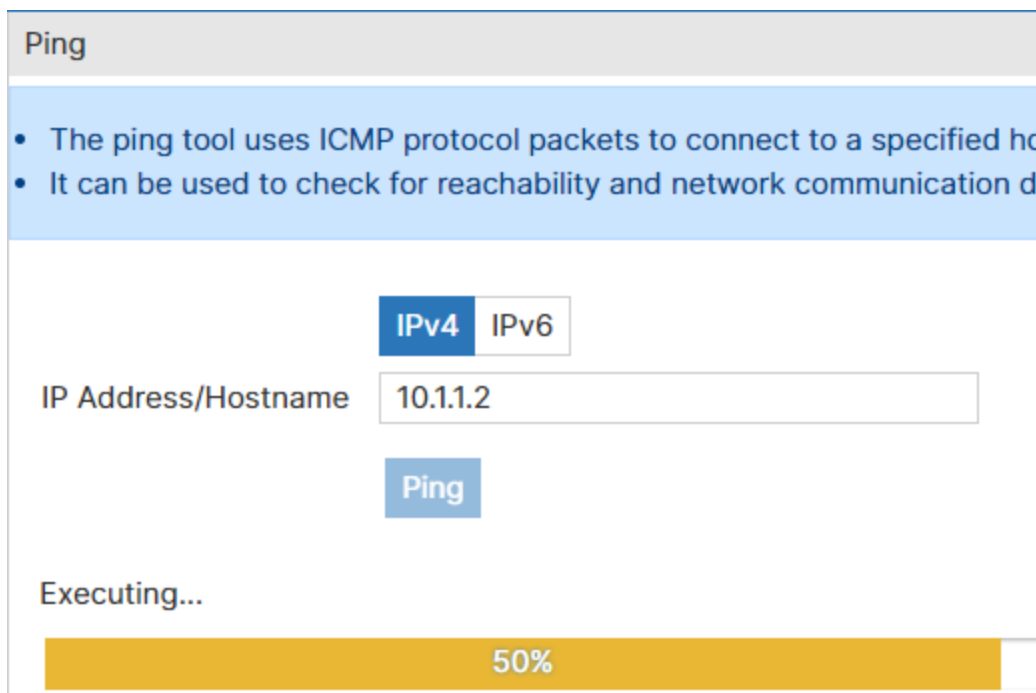
Blink LEDs

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

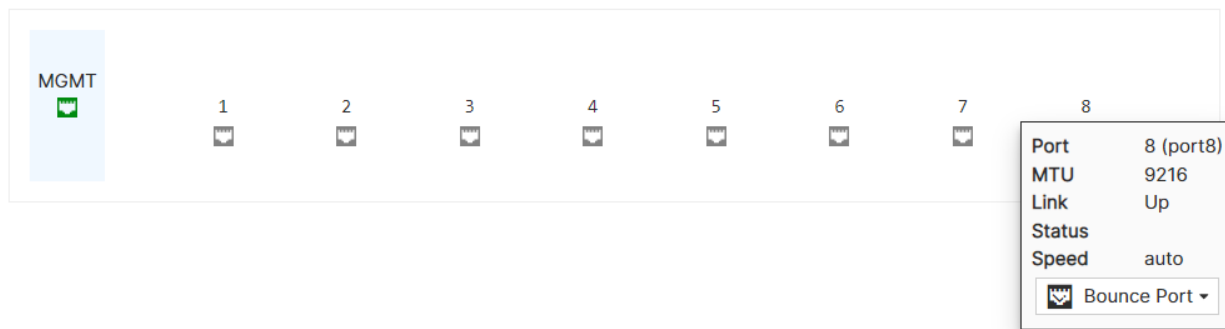
The ping command sends data packets to a specific IP address on a network, and then lets you know how long it took to transmit that data and get a response. This is used to determine reachability of the FortiSwitch to other devices on the internal or external Internet. You can conduct a ping test to 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.

- The TAC report tool executes a series of trouble shooting commands on the switch and generates a report.
- This report can be shared with customer support teams to aid in faster trouble shooting of devices. The report generation can take up to 5 minutes to complete and will generate about 2MB worth of data

Run

✔ Command Execution succeeded.

Output



Serial Number: XXXXXXXXXXXX Diagnose output

get system status

Version: FortiSwitch-108F-POE v7.2.1,build0406,220621 (GA)
Serial-Number: XXXXXXXXXXXX
Boot: Coldboot
BIOS version: 04000001
System Part-Number: P26234-01
Burn in MAC: XXXXXXXXXXXX
Hostname: S108FPTV21000078
Distribution: International

Cancel

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.

Traceroute

- The traceroute tool tracks the route that packets take in an IP network, on their way to a given host.
- This tool can be utilized to determine if/where packets from the switch are being dropped, on their journey to the specified destination.

IPv4
IPv6

IP Address/Hostname ?

TTL ?

Probe Count ?

Timeout(s) ?

Run

✓ Command Execution succeeded.

Output 📄 📥

```

traceroute to 10.1.1.2 (10.1.1.2), 32 hops max, 3 probe count, 5 timeout, 84 byte packets
 1  10.1.1.1  10 <cpe-172-116-10-10.socal.res.rr.com>  10.404 ms  10.736 ms  11.257 ms
 2  10.1.1.2  22.349 ms  22.180 ms  22.488 ms
 3  10.1.1.2  22.499 ms  21.270 ms  24.063 ms
          
```

Cancel

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.

Multi Path Traceroute ✕

- Multipath trace route is an advanced version of traceroute.
- It identifies routers which could be doing load balancing, on the path from the source to destination and attempts to avoid triggering load balancing on the routers wherever possible.

IPv4
IPv6

IP Address ?

Confidence Level (%) ?

95

Flow ID ?

udp-sport

Max TTL ?

30

Run

✓ Command Execution succeeded.

Output 📄 📄

```
Run mtracert to 10.1.1.1 - max-ttl: 30, flow-id: udp-sport, confidence: 95
0 root: 10.1.1.1 (0.327461 ms)
1 10.1.1.1: 10.1.1.1 (0.372209 ms)
2 10.1.1.1: 10.1.1.1 (0.417439 ms)
3 10.3.1.1: 172.16.1.1 (254.571964 ms)
```

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.

Checking the value sets the value in the switch to the value in the text field. Un-checking the value resets the value on the switch.

Port (All) Admin Global Internal Interface Management Interface Feature License

i This action is only available for FortiSwitches with firmware version v7.0.0 or higher. When applying a feature license key with a ZTC Config, the switch will reboot and stop all subsequent CLI commands to the device. Please ensure you only add one key per device and run the required command only after all other commands.

License Key

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

