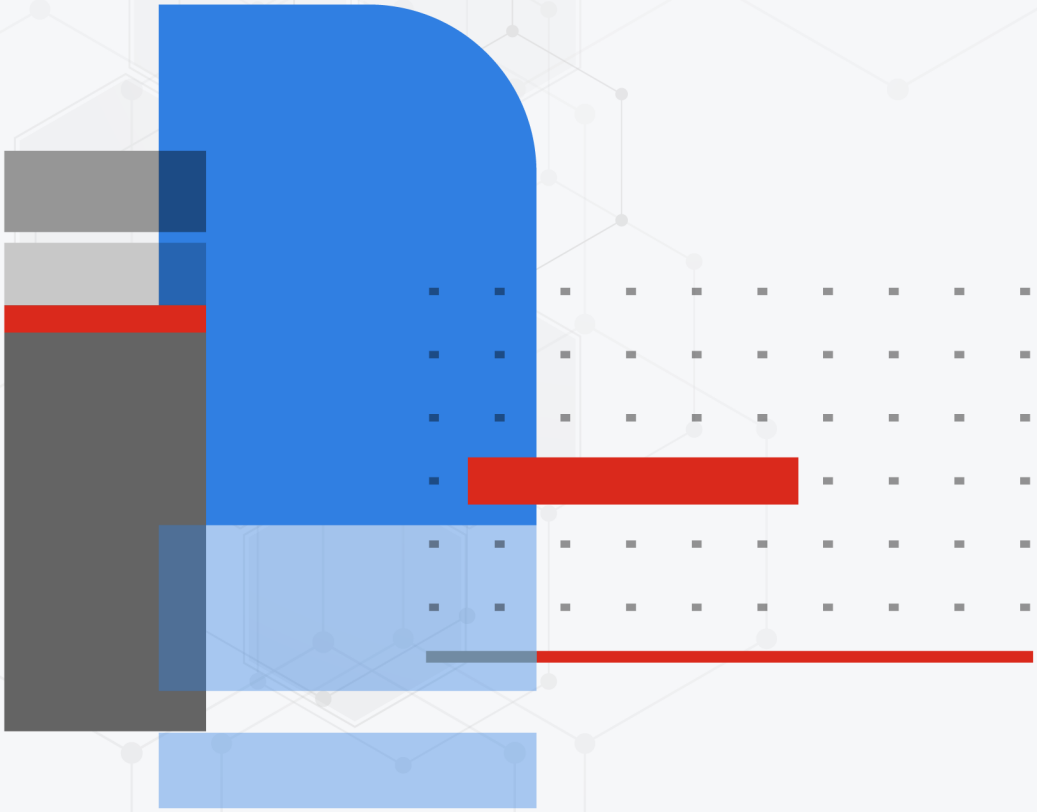
New Features

FortiLAN Cloud 24.1



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

June 20, 2024
FortiLAN Cloud 24.1 New Features
53-241-859687-20240620

TABLE OF CONTENTS

Change log

Date	Change description
2024-03-08	FortiLAN Cloud 24.1 release version.
2024-04-24	Updated New Device Support.
2024-06-20	Updated New Device Support.

Wireless

These are the new features/enhancements for FortiAPs.

SSID Configuration Enhancements

This release of FortiLAN Cloud delivers the following SSID enhancements.

Advertising Elements in Beacons

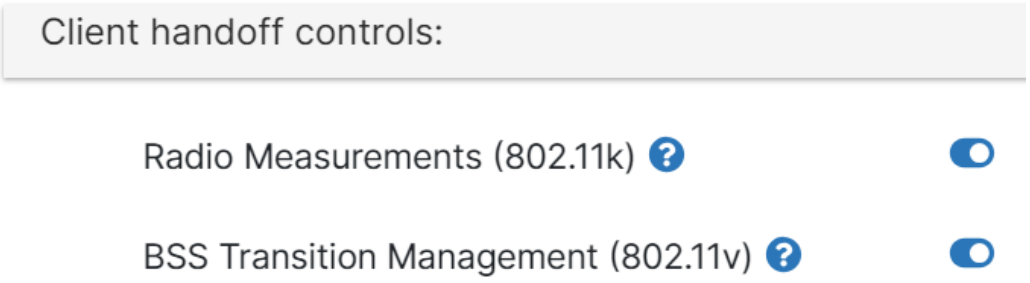
You can now enable the advertising of vendor specific elements in beacons that contain FortiAP information such as its name, model, and serial number. This enables administrators to easily identify the coverage areas using site surveys. Navigate to **Wireless > Configuration > SSID**.

Consider the following scenarios that use this feature effectively.

- The administrator is able to gradually move away from the FortiAP while continuously sniffing the beacons to determine if they can still hear from the FortiAP.
- The FortiAP are easily identified during network troubleshooting.

Segregated 802.11k and 802.11v

With this release, FortiLAN Cloud segregates 802.11k and 802.11v into standalone features that you can configure when creating an SSID. So far, the 802.11k and 802.11v features were bundled into **Voice Enterprise (802.11kv)** configuration, however, these features provide different functionality and are used in specific scenarios. This feature provides more flexibility to the network administrator to disable the network's ability to influence the roaming decision of the clients, especially, in high density deployments with a large number of FortiAPs. In cases where network planning is not good, using 802.11v may impact client connectivity. Navigate to **Wireless > Configuration > SSID**.

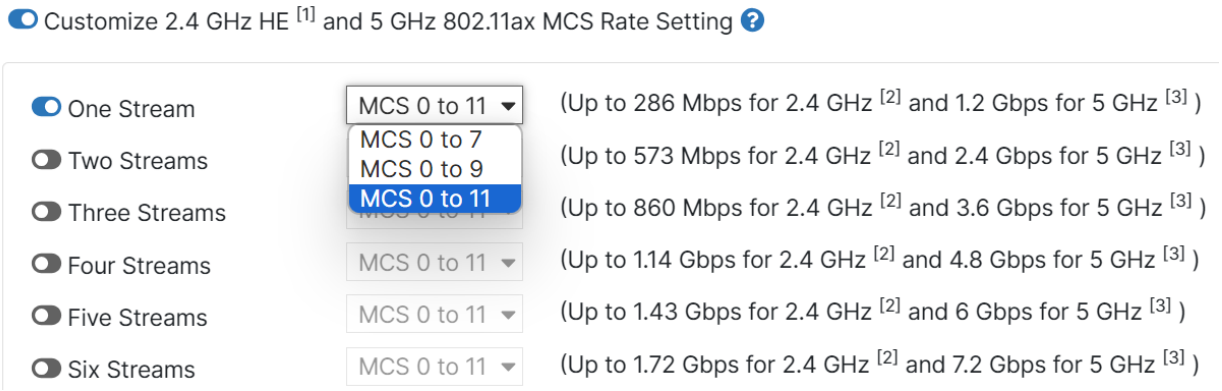


- **Radio Measurements (802.11k)** - 802.11k network assisted roaming allows a potential roaming wireless client to collect from its current AP the list of compatible neighbour APs. This saves the wireless client from performing full scan on both bands. The wireless client selects and moves to the optimal neighbour AP from the list. The 802.11k also provides support for Radio Resource Management (RRM) such as APs querying the associated wireless clients for beacon reports and perceived RSSI used to prepare the compatible neighbour AP list for wireless clients.
- **BSS Transition Management (802.11v)** - 802.11v network assisted roaming allows the wireless network to send requests to associated clients, recommending better APs to associate with while roaming. This is beneficial for both load balancing and in guiding clients with poor connectivity.
  The BSS Transition feature allows the roaming client to initiate a BSS transition query to the associated AP for a candidate list of other APs it can re-associate with, the associated AP responds with a BSS transition request containing the requested AP list. The AP can also send an unsolicited BSS transition request to the client. The client can accept the request and re-associate with the suggested APs or it can reject the request and continue its association with the current AP.

Note: **The Voice Enterprise (802.11kv)** configuration is no longer available. If you were using the 802.11kv setting in the previous release, then in the current version both 802.11k and 802.11v will be enabled.

Support for 11ax Data Rates

This release of FortiLAN Cloud supports 11ax data rates in SSID configuration. In the section **Customize 2.4 GHz HE [1] and 5 GHz 802.11ax MCS Rate Setting**, configuration for spatial streams 1 to 8 is supported with MCS rate selection values of 0 to 7, 0 to 9, and 0 to 11. Navigate to **Wireless > Configuration > SSID**.

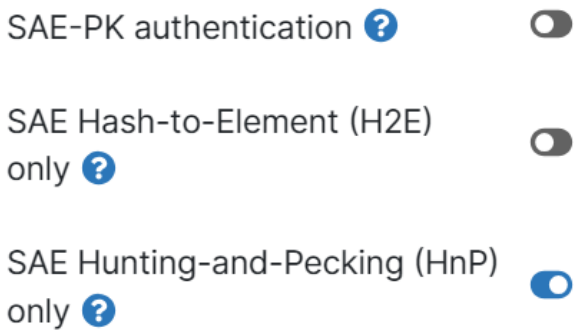


Note: This feature is supported only on FortiAPs with version 7.2.1 and above.

WPA3- SAE - HnP

The **SAE Hunting-and-Pecking (HnP) only** option is now available for WPA3- SAE authentication mode. The HnP is disabled by default and is used for PWE derivation. Sometimes, when the FortiAP operates with full WPA3-R3 compliance, some wireless clients are unable to connect to WPA3 SSIDs beaconed by the FortiAP. This issue arises as the WiFi chipset and driver on these clients do not recognize some RSN IEs beaconed by the FortiAP. To resolve this client connectivity issue, you can enable the SAE HnP option, to ensure that the client can establish a connection using WPA3 to the FortiAP.

This feature can be used only when **SAE-PK authentication** and **SAE Hash-to-Element (H2E) only** are disabled.



Note: This feature is supported on FortiAP version 7.4.2 and above.

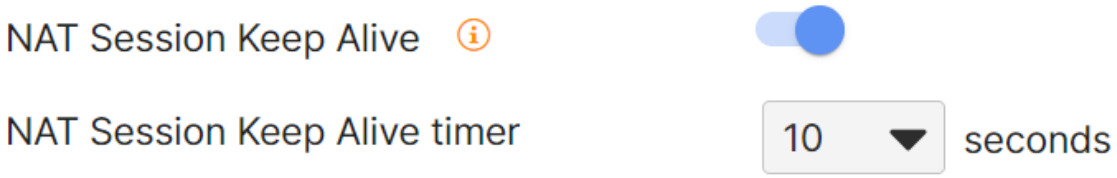
Network Settings Enhancements

The following enhancements are delivered in this release of FortiLAN Cloud.

- NAT Session Keep Alive Timer
- Managing Automatic FortiAP Reboot

NAT Session Keep Alive Timer

The FortiAP sends a probe message to the cloud servers at the configured **NAT Session Keep Alive timer** duration. This ensures NAT sessions on all intermediate devices in the network path are kept alive. This feature is especially beneficial in case of firewalls with short lived NAT sessions, that sometimes cause the FortiAPs to go offline. Navigate to **Wireless > Configuration > Network**.



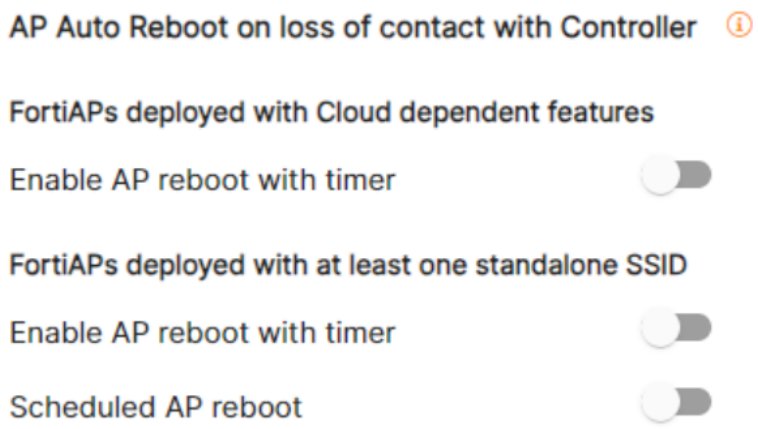
Notes:

- This feature is applied to all FortiAPs in the network.
- This feature is supported on FortiAP version 7.4.2 and above.

Managing Automatic FortiAP Reboot

This feature allows you to configure FortiAPs for an automatic reboot when they lose connection with the cloud controller. In such a scenario, this feature reduces network downtime and eliminates the need for manual intervention. If the SSIDs are configured on the FortiAP in standalone mode (such as PSK authentication), then the FortiAP does not interact with the cloud controller for authentication of wireless clients. However, in some cases (such as Enterprise authentication with cloud user/group or MAC allow lists), the SSIDs are in the non-standalone mode, that is, the FortiAP needs to interact with the cloud controller for authentication. This feature is configured separately for standalone and non-standalone SSIDs. Navigate to **Wireless > Configuration > Network**.

- **FortiAPs deployed with Cloud dependent features** - **Enable AP Reboot with Timer** - Enable the automatic reboot of the FortiAP and configure the time interval the FortiAP waits before automatic rebooting, after losing connection with the cloud controller. The valid range is 5 to 65535 minutes and the default is 60 minutes.
- **FortiAPs deployed with at least one standalone SSID** - **Enable AP reboot with timer** - Enable automatic reboot in case if there is at least one standalone SSID beaconed by the FortiAP. Enter the time interval the FortiAP waits before automatic rebooting. The valid range is 5 to 65535 minutes and the default is 60 minutes.
- **Schedule AP reboot** - Enable the FortiAP to automatically reboot at a specific time when standalone SSIDs are pushed to the FortiAP in the previous session.



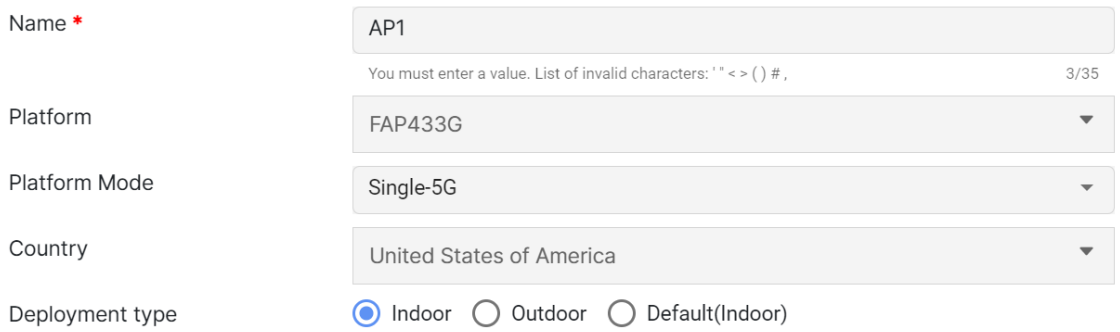
Note: This feature is supported on FortiAPs version 7.4.2 and above.

Operating Environment Classification for Channels

With this release, you can select the operating environment for channels of a specific FortiAP, whether indoor or outdoor. This feature facilitates compliance with the access point placement regulations enacted in different geographical locations. You can now override the default placements of FortiAPs when configuring a FortiAP

Platform Profile. This feature optimizes Wi-Fi performance and is beneficial in different deployment scenarios, such as the following. Navigate to **Wireless > Configuration > Operational Profiles > FortiAP Platform Profile**.

- Indoor APs are enclosed in outdoor enclosures, mimicking the form factor of their outdoor counterparts.
- Outdoor APs are temporarily mounted in indoor hangers for testing or maintenance purposes.



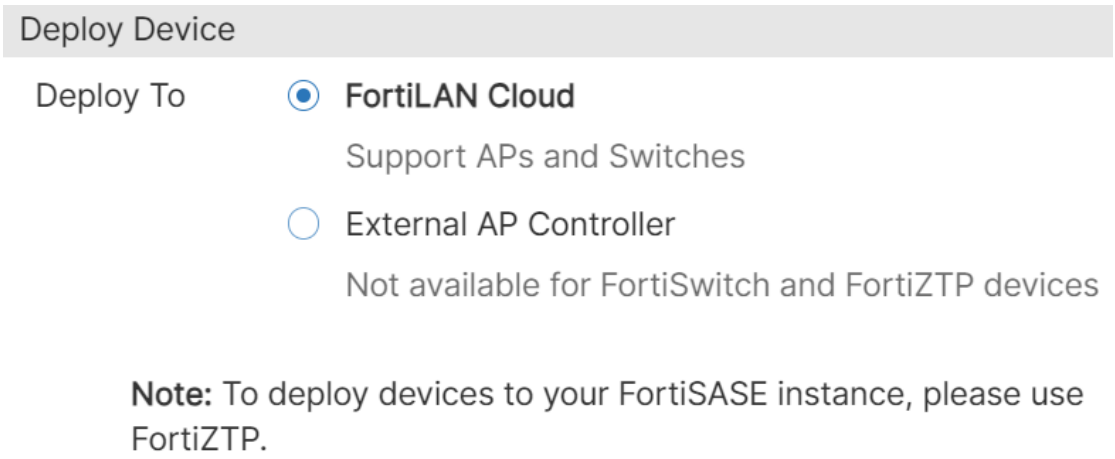
This feature is available only for these FortiAP models, FAP433F , FAP433G , FAP234F, FAP432FR,FAP432F and FAP234G.

Switch

These are the new features/enhancements for FortiSwitches.

Deploying FortiSwitch to FortiSASE

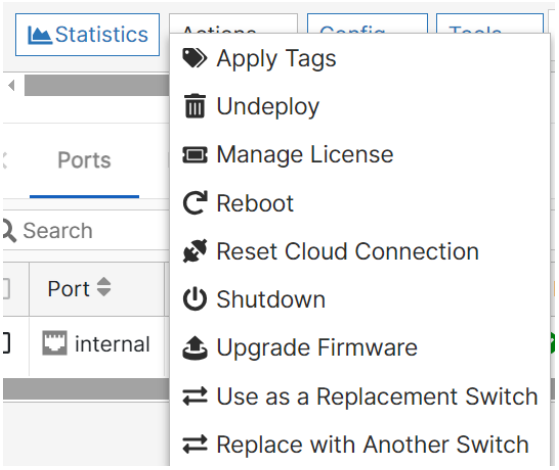
You can now deploy FortiLAN Cloud managed FortiSwitches to FortiSASE via FortiZTP.



Note: To deploy devices to your FortiSASE instance, please use FortiZTP.

Reset Cloud Connection

The **Reset Cloud Connection** action is now available for FortiSwitches. This feature facilitates recovery of devices that are not able to maintain a coherent connection with FortiLAN Cloud. When used, the FortiSwitch disconnects and re-joins the FortiLAN Cloud.


Statistics
Apply Tags
Undeploy
Manage License
Reboot
Reset Cloud Connection
Shutdown
Upgrade Firmware
Use as a Replacement Switch
Replace with Another Switch
Ports
Search
Port
internal

FortiLAN Cloud

These are the new features/enhancements for FortiLAN Cloud.

New Device Support

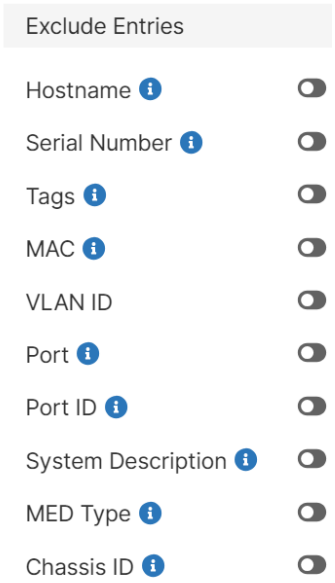
The following new devices are supported in this release. For more information, see FortiAP Series.

- FAP-441K
- FAP-443K

Device/Client Query Enhancements

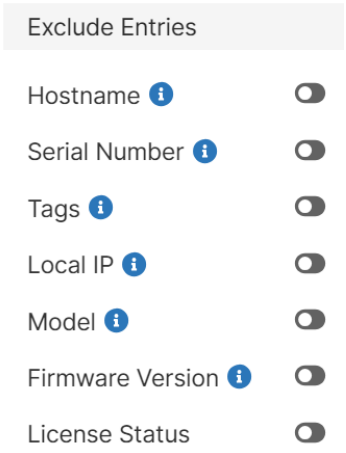
For querying wired clients, the following entries are now additionally supported. Navigate to **Clients > Adv. Filters**.

- Port
- Port ID
- System Description
- MED Type
- Chassis ID



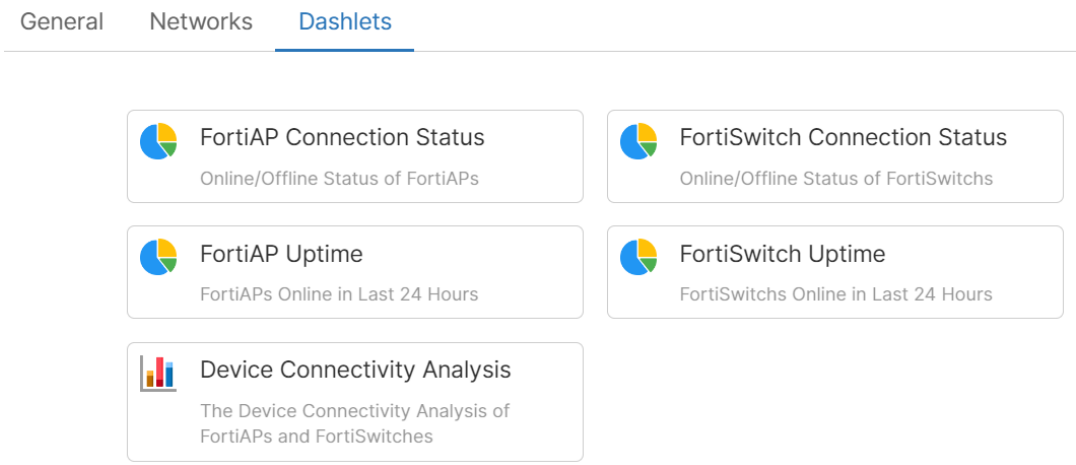
For querying FortiSwitches, the following entries are now additionally supported. Navigate to **Devices > Deployed Devices > Adv. Filters**.

- Model
- Firmware Version
- License Status



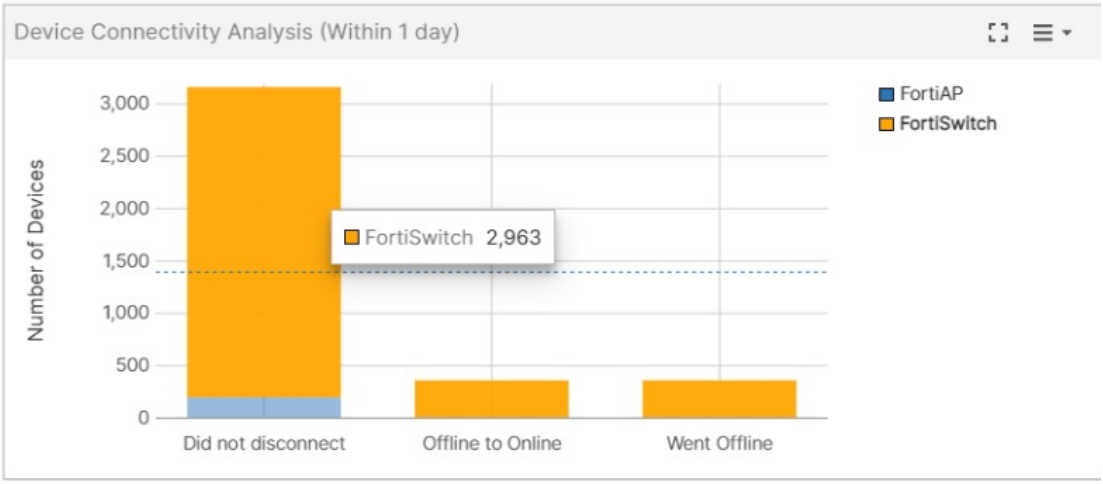
Device Connectivity Analysis and Reports

The device connectivity analysis graphs for FortiAPs and FortiSwitches are added in the custom dashboards and reports. You can now add this dashlet when creating a dashboard.

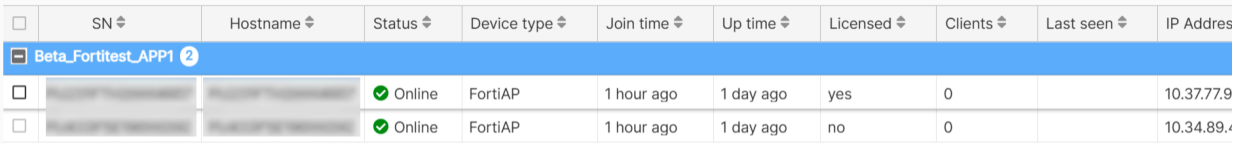


This chart displays the connectivity status of FortiAPs and FortiSwitches over the selected period of time. It provides insights into the following device statistics.

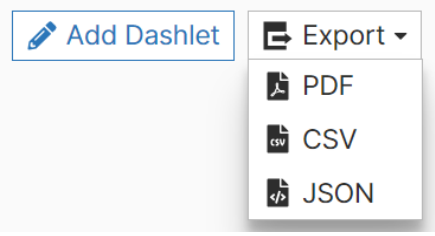
- Devices that went offline.
- Devices that went offline and then came online (re-booted, re-connected, and so on).
- Devices that did not disconnect.



Click on the bar to view the device details.



The data from the custom dashboards can be exported into reports that are supported in the PDF, CSV, and JSON formats. Select **Export > [PDF | CSV | JSON]**.


Add Dashlet
Export
PDF
CSV
JSON

www.fortinet.com