UNIVERSITAS UTPADAKA SWASTIKA
Jl. KS Tubun No.II Tangerang 15112 Banten, Telp. (021) 5589161-62 Fax. (021) 5589163
JISI
Jurnal Ilmiah Sistem Informasi
Vol. 2 No. 02 (2024)
ISSN: 3046-711X

Utilizing LED Usage on FortiManager Device as a Software Monitoring Indicator for Fortinet Access Points

Moh Alfaujianto

Utpadaka Swastika University, Tangerang, Indonesia, 15112
E-mail: moh.alfaujianto@utpas.ac.id

Accepted: October 29, 2024 | Published: October 31, 2024

ABSTRACT

In today's digital era, stable connectivity and fast troubleshooting are crucial to support corporate, academic, and research activities. One important component in network infrastructure is the access point (AP) which functions to provide a wireless connection. With the large number of Access Points (AP) provided by campuses or offices, it is required to be easy to monitor and troubleshoot all Access Point (AP) devices. Fortigate, as a solution provider, offers access point and switch monitoring features using LED Usage. This study aims to explain how access point monitoring can be implemented effectively through the FortiManager device and is important to ensure that network devices are functioning properly. FortiManager devices can monitor switches that are connected with active or inactive status, how many active access points are on each switch are monitored, all of which clients are connected to the network can be monitored. Thus, FortiManager devices are very much needed by administrators and network technical teams to facilitate monitoring and troubleshooting.

KEYWORDS: FortiManager Device, Monitoring, LED usage, Computer Network

1. Introduction

Currently, there are many hardware monitoring software to make it easy for information technology personnel to easily monitor the performance of the devices they manage. Such as Grafana, Prometheus, Nagios, Manage Engine, PRTG Network Monitoring and there are still many monitoring software available today, both paid and free software.

Of the many monitoring software available, the average monitoring software is able to monitor network performance, if there is a network anomaly or not, the device is on or off, but not all of this monitoring software is able to reach the indicator level at the Access Point (AP), this is very important because with information about the condition of the Access point, network administrators or network technicians can easily analyze existing problems. Namely by paying attention to the light indicators at the access point.

A different case is what if all indicators are off (inactive) but all internet can be accessed, seen from the active monitoring software there are no obstacles, laptops or PCs can be connected using wifi communication, likewise with the Bluetooth indicator not active but the laptop or PC Bluetooth is connected, this problem makes the network administrator team and technicians feel very difficult to find where the real problem is, because looking at the monitoring software it looks normal there are no obstacles only in the field the Access Point looks constrained damaged or all the indicator lights are off.

Fortigate, as a solution provider, offers access point and switch monitoring features using LED Usage. This study aims to explain how access point monitoring can be implemented effectively through the FortiManager device and is important to ensure that network devices are functioning properly.

FortiManager devices can monitor switches that are connected with active or inactive status, how many active access points are on each switch are monitored, all of which clients are connected to the network can be monitored. Thus, FortiManager devices are very much needed by administrators and network technical teams to facilitate monitoring and troubleshooting

2. Literature Review

In a computer network there are several components that support each other to become a computer network that suits the needs and supports performance. Starting

with network topology, supporting components and menus on the software provided by the Fortigate device.

2.1 Computer Network

A computer network is a connection of a number of devices that can communicate with each other (a network is an interconnection of a set of device capable of communication). The devices referred to in this definition include all types of computer devices (desktop computers, laptops, smartphones, tablet PCs) and connecting devices (routers, switches, modems, hubs).[1]

Wireless Network

A wireless network is a computer network that does not use network cables (UTP, Coaxial, or Fiber Optic), but uses electromagnetic signals.[1]

2.2 Network Topology

Computer network topology is defined as a technique, method and rule for assembling and connecting various computers and other connected devices into a computer network, thus forming a geometric relationship. This topology is a design, which can then be implemented directly through a number of connecting hardware on a computer network.[1]

2.3 Computer network components

a. Router
   Is a hardware device on a computer network that functions in the Routing process to determine the route taken by data packets from the sending computer to the receiving computer.[1]
b. Switch
   Is a connecting hardware device in a computer network that is currently used more than a hub.[1]
c. Access Point
   A PC network hardware device that connects wireless devices (does not use cables) to a local internet network using technologies such as wireless, WiFi, Bluetooth, and others.

2.4 FortiManager Device

FortiManager virtual appliances offer the same powerful management features as FortiManager hardware-based appliances, with the addition of a stackable license model that enables easy growth with your network environment. Fortinet virtual appliances allow you to deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized FortiManager platform.[2]

2.5 Feature Visibility

The policy and objects that are displayed on the *Policy & Objects* pane can be customized, and Policy Packages and object configurations can be displayed on a single pane.

To adjust the policies and objects that are displayed, go to *Tools* > *Feature Visibility*.

The options on or off (visible or hidden). To turn on an option, select the checkbox beside the option name. To turn off an option, clear the checkbox beside the option name. You can turn on all of the options in a category by selecting the checkbox beside the category name. For example, you can turn on all firewall objects by selecting the checkbox beside *Firewall Objects*. You can also turn on all of the categories by clicking the *Check All* button at the bottom of the window.[3]

2.6 FortiAP

FortiAP devices are thin wireless access points (AP) supporting the latest Wi-Fi technologies (WiFi-5 and WiFi-6) and the demand for plug and play deployment. FortiAP devices come in various form factors (desktop, indoor, outdoor, or wall jack). FortiAP has three wireless management topologies (integrated, FortiLAN Cloud, or dedicated controller).[4]

UNIVERSITAS UTPADAKA SWASTIKA
Jl. KS Tubun No.II Tangerang 15112 Banten, Telp. (021) 5589161-62 Fax. (021) 5589163
JISI Jurnal Ilmiah Sistem Informasi
Vol. 2 No. 02 (2024)
ISSN: 3046-711X

2.7 **FortiAP** Profiles

The profile specifies details such as the operating mode of the device, SSIDs, and transmit power. Custom AP profiles can be created as needed for new devices. To view AP profiles, ensure that you are in the correct ADOM, go to AP Manager > WiFi Profiles, and select AP Profile in the tree menu.[5]

3. Research Methods

For this research method, the author conducted direct observation of the steps related to the topic taken. Each step of the testing and observation results was directly recorded by the author, through observation activities carried out at the Kemdikbud-Directorate of Culture Archive Building, Ministry of Education, Culture, Research, and Technology, the source of the problems faced by the Film Directorate at 6, Jl. Puloraya IV No. 34, RT.6 / RW.1, Petogogan, Kec. Kby. Baru, South Jakarta City, Special Capital Region of Jakarta 12170. In addition to carrying out the above activities, the author also conducted a literature study through literature that supports this research.

4. Results and Discussion

The current running topology, hardware, and also ISP in the Ministry of Education and Culture Archives Building-Directorate of Culture are as follows:

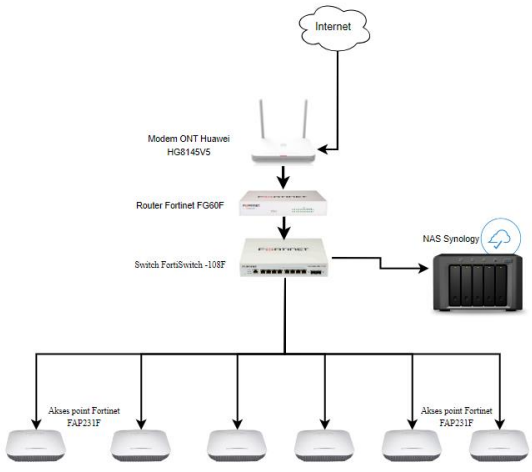

Figure 1. Existing topology in the Archives Building of the Ministry of Education and Culture-Directorate of Culture

From the topology above, there is one ISP (internet service provider) input using Telkom then entering the Huawei ONT modem, after the modem is continued to the Fortigate FG60F Router after entering the router is continued to the FortiSwitch -108F Switch and distributed to one Synology NAS and 6 Fortinet FAP231F access points and from these access points are distributed again to the end points of network devices, namely personal computers, laptops, and mobile phones.

Table 1. Network Hardware

No.	Hardware
1.	Modem ONT Huawei HG8145V5
2.	Router Fortinet FG60F
3.	Switch FortiSwitch -108F
4.	Akses point Fortinet FAP231F
5.	Komputer dan Laptop
6.	NAS Synology
7.	Handphone

The software used is as follows in the table.

Table 2. Network Software

No.	Software
1.	Window 11 Pro
2.	Mac OS
3.	Linux Ubuntu
4.	DSM Synology

4.1 Implementation

Implementation on the FortiManager Device software owned by FortiGate Next-Generation Firewall 60F (NGFW), login to the FortiManager Device application, the display is as shown in Figure 4.1 below.

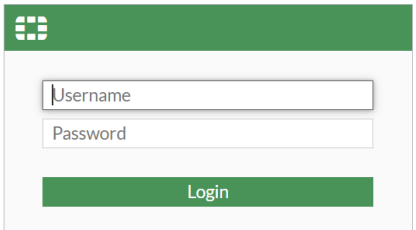

Figure 2. Login screen to FortiManager Device

UNIVERSITAS UTPADAKA SWASTIKA
Jl. KS Tubun No.11 Tangerang 15112 Banten, Telp. (021) 5589161-62 Fax. (021) 5589163
JISI Jurnal Ilmiah Sistem Informasi
Vol. 2 No. 02 (2024)
ISSN: 3046-711X

After successfully logging in and being on the FortiManager Device dashboard display, as shown in the following image:

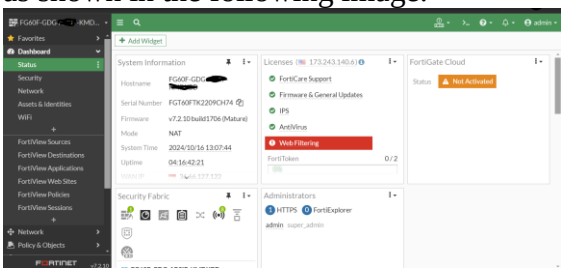

Figure 3. Fortigate FG60F Status Dashboard

After successfully logging in and on the Dashboard display, then select the Wifi & Switch Controller > FortiAp Profile > Operation Profiles menu, the display will look like the following image:

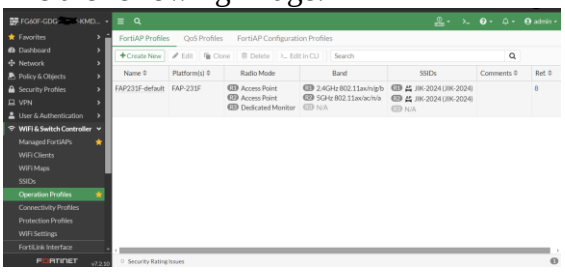

Figure 4. FortiAP Profile Menu Display

Select the existing SID name and click so that the edit menu becomes active then as in the following image:

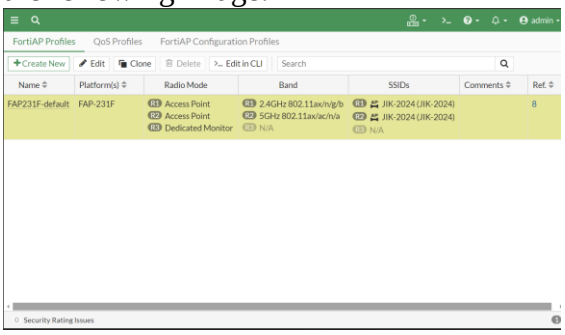

Figure 5. Selected SSIDs

If you click on the edit menu, then scroll down to select the advanced settings menu as shown below:

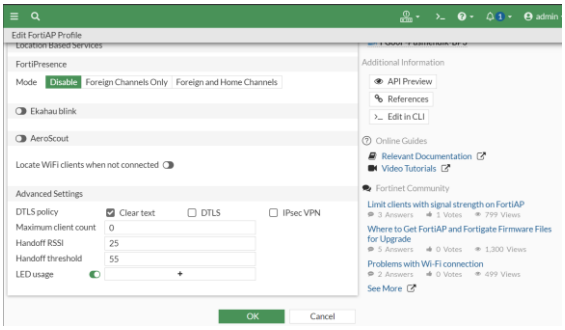

Figure 6. Advance Settings menu

In the display above, the advance setting menu and LED usage are in active condition by default. Here, the researcher conducted a trial by deactivating the LED usage status so that the display is as shown in the following image:

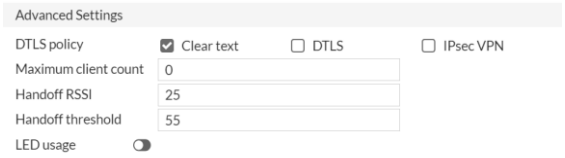

Figure 7. Inactive LED usage Indicator Status

With the Inactive condition on LED usage, it affects all access point light indicators to be inactive even in normal conditions, meaning that the AP can be accessed as usual without any problems. However, if the support technician team or network administrator sees this condition, it will be difficult to find out where the problem lies, considering that the AP is functioning as usual but the indicator shows something unusual. At the end of this study, the researcher returned the default active LED usage condition as shown in the following image:

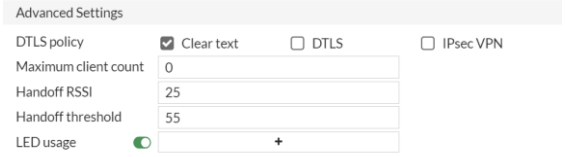

Figure 8. Active LED usage Indicator Status

By activating LED usage, all indicators on the access point come back to life and provide indicator information according to their function.

If the advanced setting menu is not displayed in the FortiAP profile menu, the feature must be activated first in the system menu > feature visibility > then select the advanced setting menu to activate as shown in the following image:

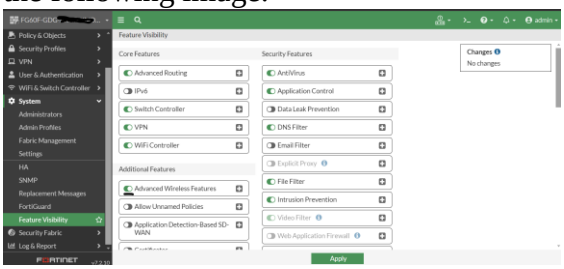

Figure 9. Activating the Advance Setting Menu

5. Conclusion

From this research, a conclusion was obtained that with the FortiManager Device system, network administrators and technicians can easily monitor the condition of network devices such as routers, switches, and access points up to the indicator function on the Access point. One very interesting finding from this research is the operation profiles in one of its sub-menus is the LED Usage, if the condition is on, the indicator on the access point will light up and if the indicator is off, the indicator on the access point will turn off, but it does not reduce the function of the access point.

References

[1] I Putu Agus Eka Pratama "Handbook Jaringan computer, teori dan praktik berbasis open source" Bandung: Informatika 2015

[2] https://www.avfirewalls.com/FortiManager-Virtual-Appliances.asp

[3] https://docs.fortinet.com/document/fortimanager/7.6.0/administration-guide/928220/ feature -visibility

[4] Datasheet fortigate-fortiwifi-60f-series

[5] https://docs.fortinet.com/document/fortiap/7.6.0/fortiwifi-and-fortiap-configuration-guide/809346/operations-profiles-entry

[6] Sari Dewi , Adam Iqbal Islami, Implementasi Web Filtering Menggunakan Router Fortigate FG300D, INSANtek – Jurnal Inovasi dan Sains Teknik Elektro**,** Volume 2 No. 1 Mei 2021.

[7] Erwin Dwi Setiawan , Ridwansyah , Mugi Raharjo, Perancangan Keamanan Jaringan *Next Generation Firewall* Menggunakan *Router Fortinet* Pada Pt. Alodokter Teknologi Solusi. Jurnal Informatika Terpadu Vol. 9 No. 1 Maret 2023.