



Controlling SSID proliferation for better Wi-Fi performance

2024

Secure • Authenticate • Automate • Simplify

www.cloudi-fi.com


Wi-Fi network proliferation - The enterprise network manager perspective

Because of the exponential demand for connectivity and the rapidly increasing need for larger bandwidth capacity, overseeing the Wi-Fi management spectrum is critical, especially for complex multi-site organizations.

The enterprise Wi-Fi must support various usages, often requiring too many SSIDs. Indeed, each usage requires its own network (Corporate devices, guest, critical IoT, facility IoT, BYOD, etc.), degrading the global performance of the network, ranging in severe instances, to approximately 40% bandwidth loss in 2.4GHz networks.

Concurrently, the need for improved cyber security requires individualized user profiles and usage history for regulatory compliance management and data privacy.

Challenges with reducing the number of SSIDs



What is an SSID?

An SSID or Service Set Identifier is a way to separate user profiles in Wi-Fi networks

CLLOUDI-FI

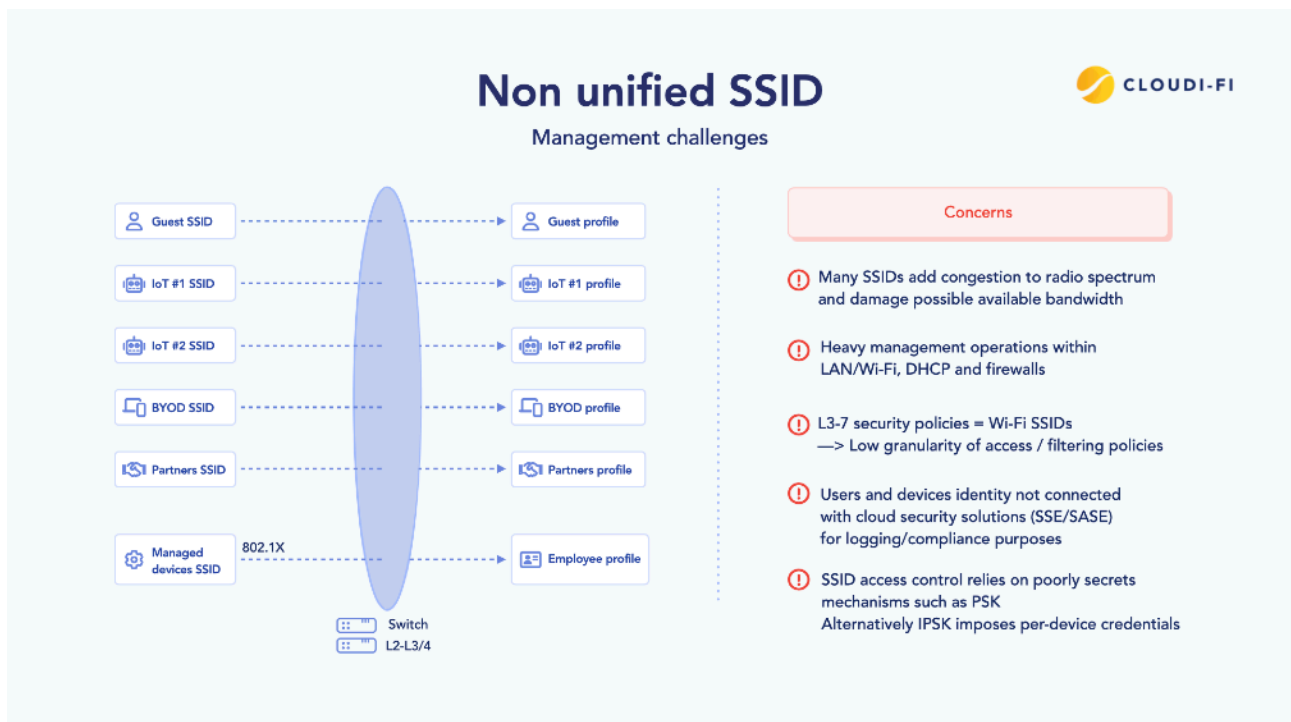
The image shows a hand holding a smartphone. The phone screen displays a list of Wi-Fi networks under the heading 'Wi-Fi Networks'. The list includes: 'Corporate - Guest', 'Corporate - BYOD', 'Corporate - Employee', 'Corporate - CCTV', 'Corporate - IoT', and 'Corporate - Lobby'. Each network name has a toggle switch to its right, all of which are currently turned off. The background of the slide is dark blue with a white shirt cuff visible at the bottom left.

SSID stands for Service Set Identifier. It's a wireless network name. Multiple SSIDs typically represent different network access levels and differentiated authentication types in a corporate environment. In the case of enterprise Wi-Fi management, such a practice is especially useful for segmenting user classes. It's considered a must within the scope of layer 2 local area networks.

Challenges caused by multiple SSID management

Network usage is rising in both quantity and diversity of usage.

Connected devices become globally prevalent, and the Wi-Fi network is their door to the Internet so they can operate properly. However, their access to the local network has to be secured, and the Internet access must be profiled to the nature of the device. This causes the creation of multiple SSID(s) per category of devices to ensure appropriate security policies. In addition, BYOD (Bring Your Own Device) strategies have gained widespread acceptance, and electronic handheld devices have proliferated among all employees and consultants. Those unmanaged computers and smartphones have the exact requirements as connected devices; they should not be connected to the corporate network but have secure access to the Internet. As a consequence, they usually require additional dedicated SSID(s)

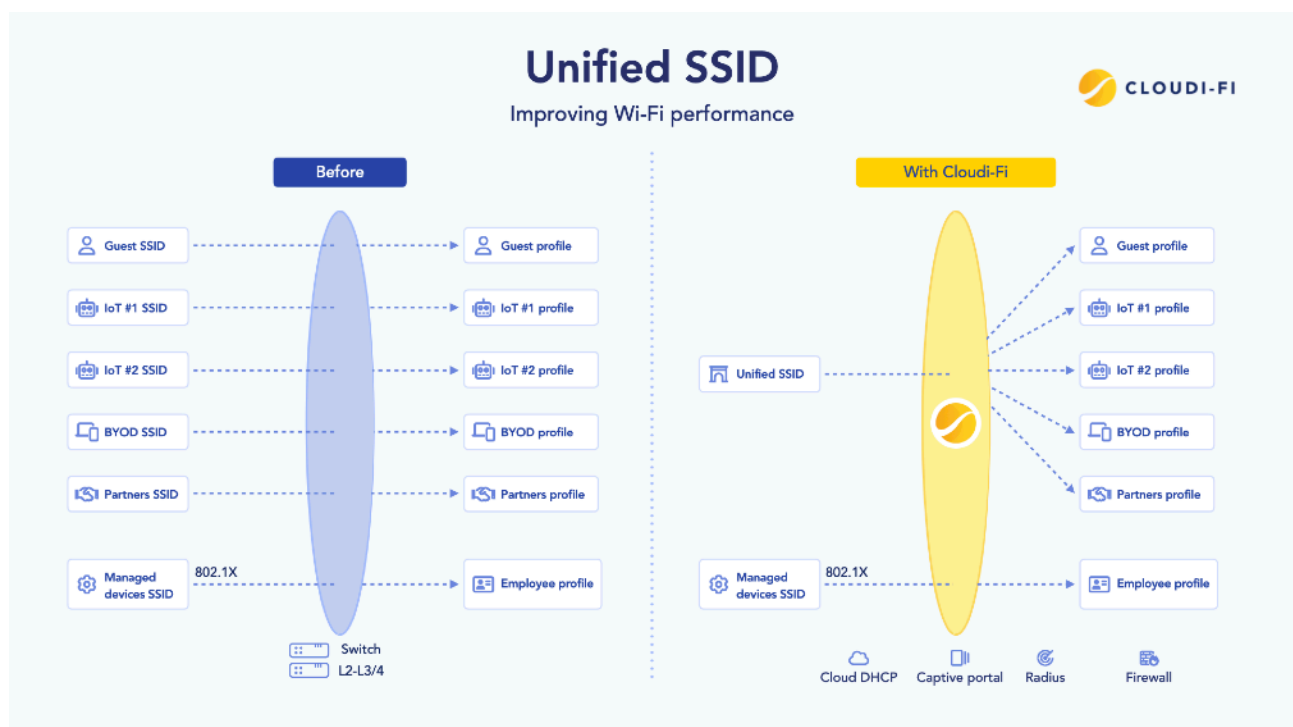


Despite its advantages, the practice has considerable drawbacks. From a radio frequency (RF) spectrum standpoint, numerous SSIDs engender interference and congestion. Each additional SSID introduces overhead to the wireless spectrum, potentially precipitating a decline in overall network performance and dependability. With recent Wi-Fi 6, some improvements, i.e., BSSID, have been brought to help limit these drawbacks. However, not all devices can support these. Furthermore, the administration and upkeep of many SSIDs impose a significant operational burden, requiring a substantial investment of time and resources on the networking infrastructure and IT management sides.

The imperative to mitigate these challenges underscores the significance of diminishing the number of SSIDs for optimizing wireless functionality. This contributes to an amelioration of the velocity and dependability of the wireless network. Additionally, a rationalized SSID framework simplifies network administration, facilitating streamlined troubleshooting procedures and imposing security policies.

Solution overview

How does Cloudi-Fi address the multiple SSID management challenge?



Cloudi-Fi Cloud Identity Platform addresses this challenge by minimizing Wi-Fi overhead and streamlining network infrastructure management. In a zero-trust context where the Internet has become the space for all applications, the user's gatekeeper is moved within the cybersecurity platforms.

Transforming the Wi-Fi access control and DHCP fingerprinting

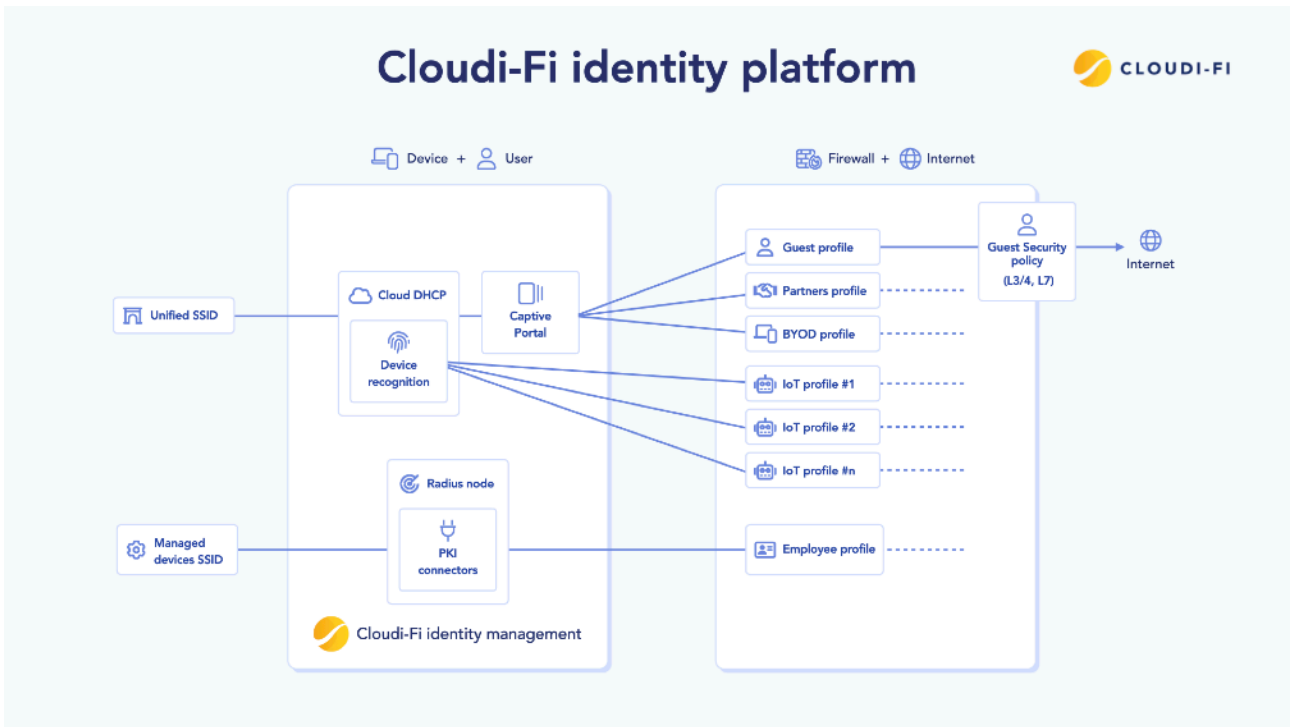
Cloudi-Fi Cloud Identity Platform transforms Wi-Fi access control by shifting focus from the conventional SSID segregation layer to a sophisticated identity paradigm, simplifying complex network Wi-Fi Management. By incorporating technologies like captive portals and DHCP fingerprinting, the Cloudi-Fi solution surpasses the basic segregation of devices and users by broadcast domains. Instead, it introduces a holistic approach, isolating them at the physical layer while assigning access rights at the security layer. This unique approach is not confined to access points but extends to firewalls, cloud-based firewalls, and proxies.

One platform to identify all untrusted devices at scale

Cloudi-Fi all-encompassing strategy applies to users, visitors, partners, BYODs (Bring Your Own Devices), and IoT (Internet of Things). Each entity undergoes individual identification and authentication, resulting in the allocation of a unique security profile tailored to its specific needs. 802.1x might persist solely for employee devices with specific local access policies and certificate-based authentication.

The Cloudi-Fi cloud-based Captive portal technology ensures users and devices are authenticated before network access, heightening overall security.

Simultaneously, DHCP fingerprinting identifies devices based on unique characteristics, enhancing the precision and granularity of access control. Departing from traditional Wi-Fi gatekeeping signifies a notable advance in network security, offering a more nuanced and flexible approach that enables finer user profiling and increased compliance.



Answering the ever-evolving landscape of network devices

Whether overseeing access points, firewalls, or cloud-based security measures, Cloudi-Fi's inventive approach ensures access control is robust and adaptable to the evolving landscape of network-connected devices and users.

By adopting an identity-centric model, Cloudi-Fi establishes a new standard in Wi-Fi access control, promoting a more secure and dynamic network environment.

Simplifying cyber identity security

Cloudi-Fi solutions move the identity paradigm from a simple SSID or switch port to a true user and device perspective. Depending on the user type, different identity providers are available, from social networks for visitors to corporate directories for employees' BYOD. Within DHCP, IoTs are attached to security profiles based on dynamic device recognition and static fingerprinting. This identity is then leveraged within the corporate security stack.

Infrastructure vendor agnostic

Within that infrastructure, the vendor-agnostic approach that Cloudi-Fi has been

developing and maintaining enables corporations to deploy these identities within their local firewalls, a tunnel from distributed SD-WAN into cloud security, or Wi-Fi access points. Our integration with significant firewall vendors and Cloud security solutions automatically transforms all legacy unauthenticated traffic into identified and profiled traffic. The visibility and control that were loose and restricted to a per-SSID/VLAN view now becomes an end-to-end cybersecurity object, giving control back to the IT administrators while freeing the radio infrastructure from SSIDs and beaconing overhead.

This unique model brings dedicated user security profiling and compliance on top of captive portal features like targeted marketing. Enabling this identity from our cloud platform within the physical location security stack not only brings better profiling capabilities and granularity but also leverages the local internet security and breakout through the firewall or cloud proxies. The corporate WAN is then discharged from that traffic.

In summary, splitting the Wi-Fi space with SSIDs was a compulsory choice. It still led to performance dramas and is now superseded by security capabilities at the higher levels of the cyber security stack.

Benefits of reducing the number of SSIDs

Reducing the number of SSIDs in complex multi-site organizations offers several significant benefits, enhancing efficiency and security. Cloudi-Fi Identity Platform declutters the WiFi spectrum, increasing bandwidth and improving network performance.

Secondly, this approach enables detailed tracking of compliance history for each user and device, ensuring adherence to international privacy laws at scale. Integrating Zero Trust Network Access (ZTNA) and firewall capabilities into security profiles fortifies network defenses.

Thirdly, it allows for unlimited granularity in security profiles, enabling more precise and tailored security measures.

Lastly, organizations can streamline authentication processes by leveraging corporate identity providers, enhancing user convenience, and bolstering identity management.