Microsoft Windows Autopilot: Seamless onboarding and deployment with Cloudi-Fi

2024

Secure · Authenticate · Automate · Simplify

www.cloudi-fi.com

What is Windows Autopilot?

Windows Autopilot simplifies the Windows device lifecycle for both IT and end users, from initial deployment to end-of-life using Windows cloud-based services. Windows Autopilot is a collection of Windows technologies used to set up and pre-configure, repurpose, or recover Windows devices.

This solution enables the IT department to achieve these goals with little to no infrastructure to manage. In addition, it enables IT administrators to customize devices without physically handling them; the end-user can launch the process as long as the device has access to Microsoft public URLs and IPs.

Challenges of implementing Windows Autopilot in an enterprise network

Windows Autopilot can be used multiple times during the life cycle of a Windows device. The process is launched as a self-service and relies on a script requiring access to multiple URLs and IPs on the Internet.

During the process, the Windows device will pass through various states and will not be able to support enterprise authentication (such as 802.1X). Consequently, IT teams are challenged to provide Internet access to unsecured and unmanaged devices in all locations (where Autopilot can be launched).

Enabling Windows Autopilot easily on all sites

Cloudi-Fi's Access Control Platform offers seamless integration with Microsoft Autopilot to enhance user experience.
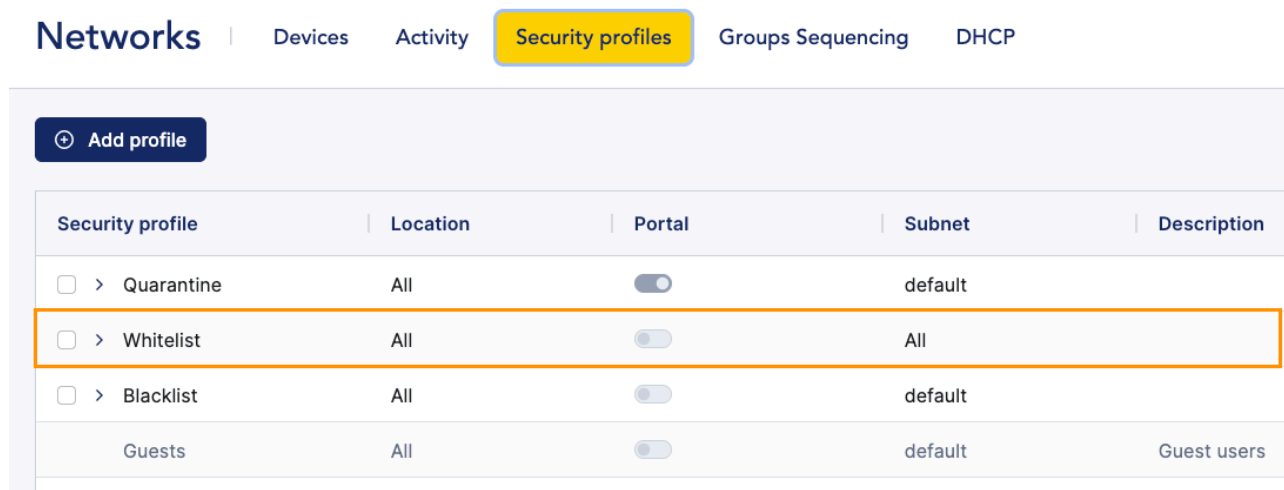
The Cloudi-Fi Cloud Identity Platform deactivates captive portals within this specific context. This feature can seamlessly integrate into any existing Guest WiFi SSID, either alongside a captive portal or on a dedicated SSID with the captive portal disabled. If integrated within the captive portal, a set of deterministic methods for device safelists should be defined, typically relying on device signatures or MAC addresses.

CLOUDI-FI

USE CASE

In conjunction with Cloudi-Fi cloud-based DHCP service, Windows devices are effortlessly recognized upon reconnection. Furthermore, for user authentication, Cloudi-Fi supports authentication for large customer systems facilitated by the SAML authentication protocol, enabling device authentication on the network. Finally, the ongoing maintenance of safe listing safelisting for Microsoft and Apple URLs/IPs is managed by Cloudi-Fi.

For multinationals with heterogeneous solutions, Cloudi-Fi can easily be deployed on all sites on various infrastructures to deliver the same capability everywhere. AutoPilot deployment with Cloudi-Fi is flexible and scalable while addressing security team concerns. See below for various deployment scenarios.

Windows Autopilot deployment (scenario 1)

Devices would be registered in bulk or individually with their MAC address as an identifier. When these devices pop up, the Cloudi-Fi DHCP server delivers an IP address belonging to a specific security policy, allowing connection to Windows Autopilot servers. This can be implemented on existing SSID.

Device MAC address whitelisting with Cloud-based DHCP service

Bulk or individual device registration to Windows Autopilot servers
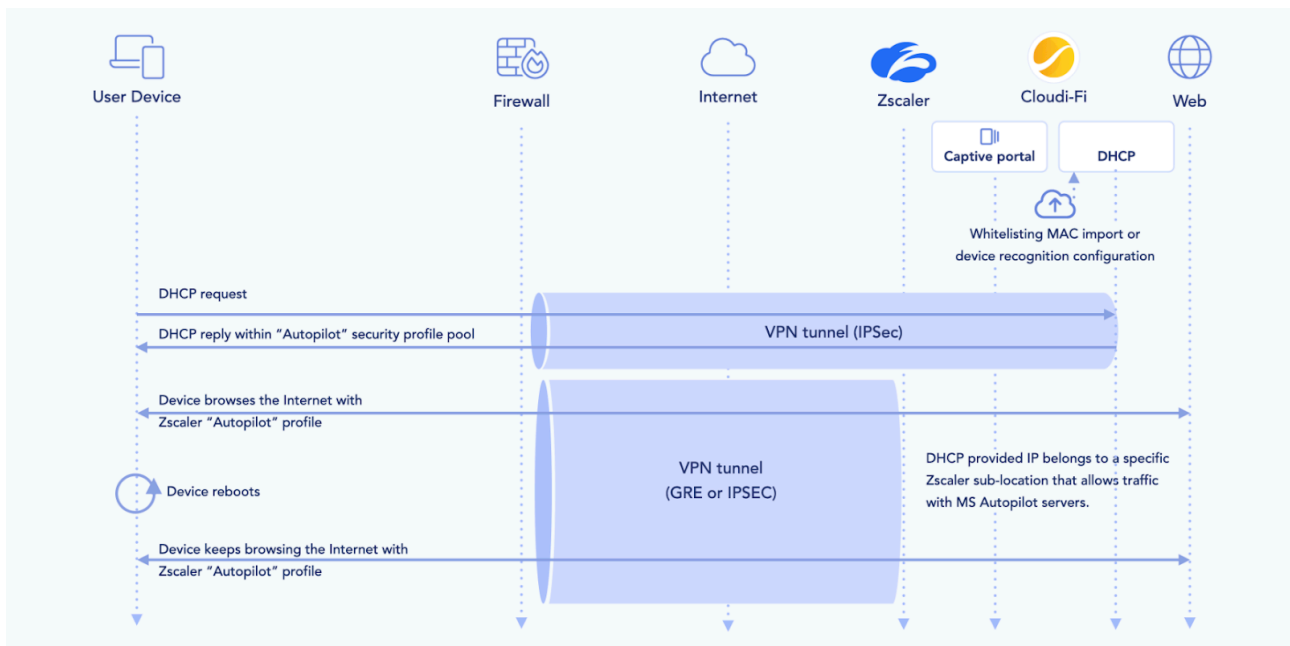
Bulk or Individual Device Registration via MAC Address for Enabled Connection to Windows Autopilot Servers without SSID Segregation
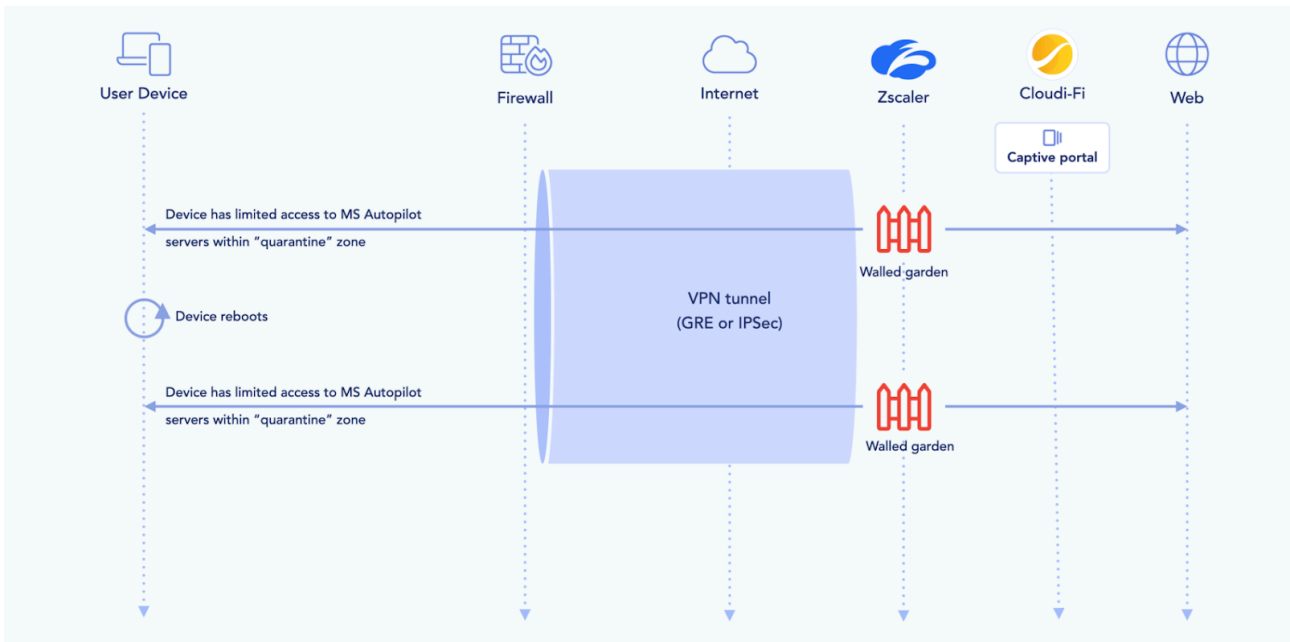
Windows Autopilot deployment (scenario 2)

All devices from the walled garden can reach Windows Autopilot servers. Whether they have identified or not, they can fetch their provisioning information. Still, the traffic to Autopilot servers is logged. An additional barrier with a specific SSID and WPA(n) PSK might be required.
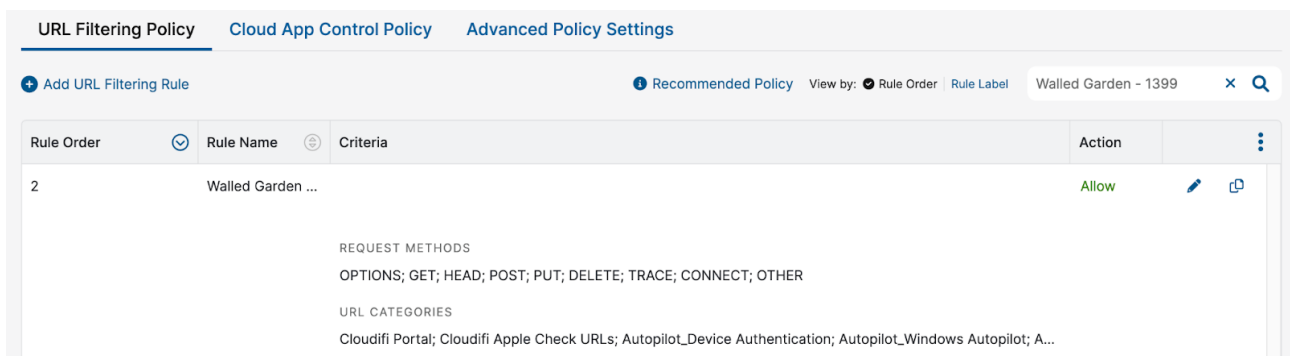
Update URL policies to allow access to Autopilot Servers before device authentication

CLOUDI-FI

USE CASE

Whitelist Windows Autopilot server

Whitelist Autopilot Servers before device authentication

Windows Autopilot deployment (scenario 3)

There is no need to dedicate an SSID; If the device can be identified via the captive portal and a company directory (e.g., Azure AD) that confirms an employee's identity, Cloudi-Fi will bind the user into a specific profile where Windows Autopilot servers can be reached. Rebooting the device would not alter the connectivity as long as the device keeps the same IP address, which can be guaranteed with a Cloudi-Fi cloud-based DHCP server.

All authenticated employees (with SAML authentication with AD) can access the internet and so AutoPilot URLs

CLOUDI-FI

USE CASE

Whitelist Autopilot servers only for internal users
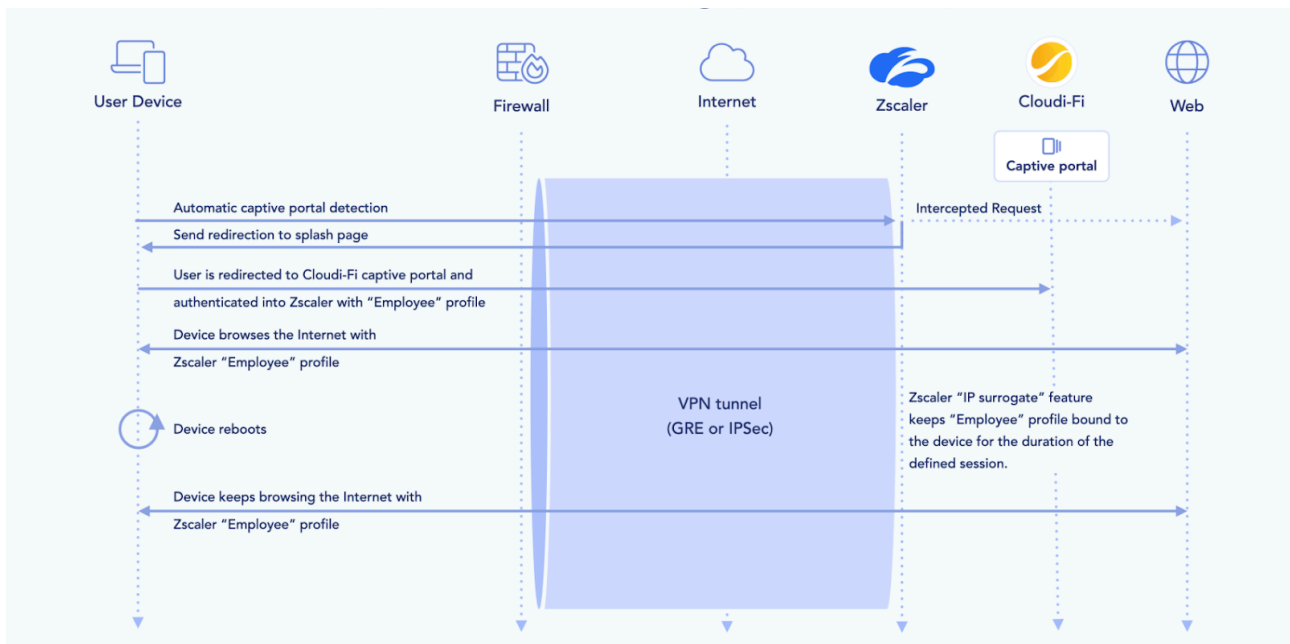
Whitelist Autopilot Servers only for internal users (authenticated through Active Directory)

Windows Autopilot users onboarding benefits

Implementing seamless Windows Autopilot using the Cloudi-Fi Cloud Identity Platform for user onboarding presents numerous benefits, effectively addressing key areas of concern for any IT department.

Firstly, it significantly reduces the time IT staff must dedicate to deploying devices by minimizing troubleshooting and support time during device setup. Secondly, the process simplifies onboarding by seamlessly reconnecting devices to the Visitors' SSID, thus avoiding the need to use the corporate network during the Autopilot onboarding process. This not only streamlines the process but also mitigates potential network congestion.

Lastly, and most importantly, it addresses security concerns effectively. The ability to enforce custom access policies during the onboarding process ensures that security is not compromised, maintaining the integrity and safety of the corporate network. Overall, these enhancements brought by seamless Windows Autopilot

significantly improve the efficiency and security of the user onboarding experience, proving to be a valuable asset for any organization aiming to optimize its IT operations.

Benefits Summary

Windows Autopilot users' onboarding with the Cloudi-Fi Cloud Identity Platform simplifies your IT operations.

- Reduces the time IT spends on deploying: minimizes troubleshooting time and overall time dedicated to supporting users during device set-up.
- Simplifying the onboarding process (transparent re-connection to the Visitors' SSID during the Autopilot onboarding process) without using your corporate network.
- Addressing security concerns through custom access policies.

Sources:

- https://learn.microsoft.com/en-us/autopilot/windows-autopilot