WINDOWS AUTOPILOT USER-DRIVEN HYBRID AZURE AD JOIN USING ALWAYS ON VPN

WHITEPAPER

Windows Autopilot User-Driven Hybrid Azure AD Join using Always On VPN

Overview of Windows Autopilot

Windows Autopilot, a component within Microsoft Intune, provides an advanced capability for the setup and pre-configuration of new devices, facilitating their swift preparation for productive use. Additionally, it enables the utilization of Windows reset, repurposing, and recovery functionalities for devices.

The Windows device life cycle becomes more streamlined with the assistance of Windows Autopilot, benefiting both IT professionals and end-users alike.

By leveraging Windows Autopilot, the overall costs and time invested by the IT team in deploying, managing, and retiring devices are significantly reduced. Furthermore, it diminishes the infrastructure requirements for maintenance, ensuring a user-friendly experience for all end-users.

Hybrid Azure AD joined devices and Windows Autopilot:

Windows 10 devices have the capability to be connected to an Azure Active Directory (AD) domain, particularly when they are owned by the company. Typically, in Bring Your Own Device (BYOD) scenarios or on devices using operating systems other than Windows 10, there is the alternative to register with Azure AD. A key distinction for users is that signing in with a Microsoft work or school account directly from the logon screen is only possible on devices connected to Azure AD.

However, introducing some complexity, Windows 10 devices can also undergo hybrid Azure AD joining. In this scenario, devices are affiliated with a Windows Server Active Directory domain while simultaneously being registered with Azure AD.

Microsoft's suite of technologies, Windows Autopilot, designed to simplify the setup of new Windows 10 devices, offers various modes. In the user-driven mode of Windows Autopilot, new Windows 10 devices can seamlessly progress from their initial state, straight from the manufacturer, to a state where they are ready to use without requiring any intervention from IT.

Always-ON VPN support for user-driven hybrid Azure AD join

The user-driven hybrid Azure AD join process in Windows Autopilot involves checking the device's ability to communicate with Windows Server Active Directory through a domain controller. However, when setting up a new device and requiring a connection to the corporate network via a virtual private network (VPN), the validation of Windows Server AD connectivity fails because the VPN has not been established on the device.

To address this issue, Microsoft has introduced a new setting that allows you to bypass the AD connectivity check when configuring a Windows Autopilot deployment profile. Instead of conducting the check, Windows 10 will restart and display the Mobile Device Management (MDM) Enrollment Status Page (ESP) regardless of whether there is connectivity to Windows Server AD.

The ESP provides updates on configuration changes occurring on the device, such as app and certificate installations. During the ESP phase, a VPN must also be installed to grant the user connectivity to the corporate network, enabling them to sign in to Windows Server AD. You have the option to install a VPN client or perform any other necessary configurations to establish VPN functionality. The condition is that the VPN connection must either be automatically established, as with a Windows 10 Always On VPN, or the VPN client must allow users to connect to the VPN server directly from the Windows 10 logon screen.

InstaSafe Secure Access (ISA) solution provides Always ON VPN connectivity for users to connect to the corporate network once the device is turned on.

InstaSafe Secure Access (ISA) Always ON

All devices will be configured with a generic ISA user profile to only permit basic AD connectivity. This generic user profile will allow users to their Windows computers as part of the Windows Autopilot process

At a later time, before handing over the computer to the end-user, the generic user profile would need to be updated/replaced with the actual end-user’s ISA user profile. This could be done manually (with Admin intervention) as well as an automated approach (without Admin intervention).

The automatic switch from the generic user profile to a specific user profile would be accomplished through a minor modification to the InstaSafe Credential Provider (ICP). This modification will enable the provisioning of user profiles as part of the sign-in process, eliminating the need for admin credentials or administrator intervention.

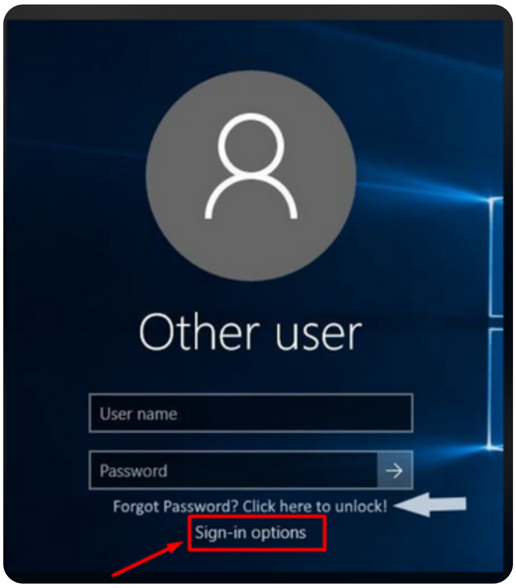
ICP will be used along with InstaSafe client configuration (clientconfig.exe) step during the Windows Logon process, making it a seamless part of the Windows Logon experience.

Step by Step Guide

1. Deployment of InstaSafe Credential Provider MSI (ICP) on End-user's System.
2. Deployment of Generic Instasafe agent on End-users System.

User Action

3. Logout the user and Click on the ‘Sign-in option’



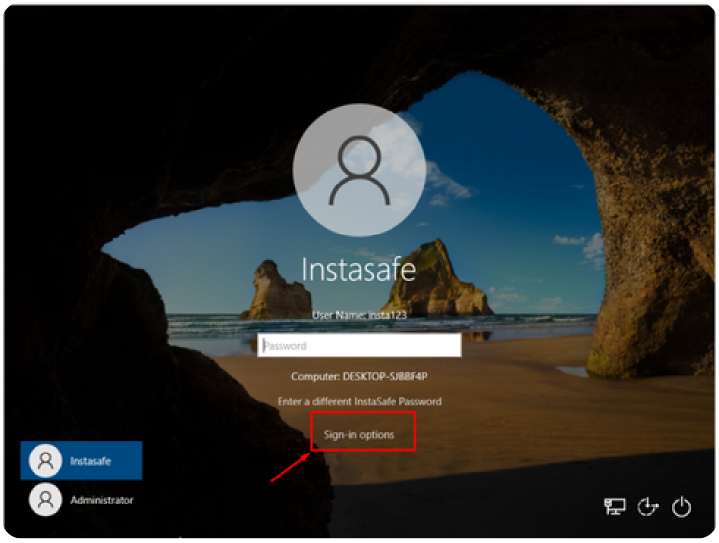
Other user

User name

Password

Forgot Password? Click here to unlock!

Sign-in options



Instasafe

User Name: insta123

Password

Computer: DESKTOP-SJBBF4P

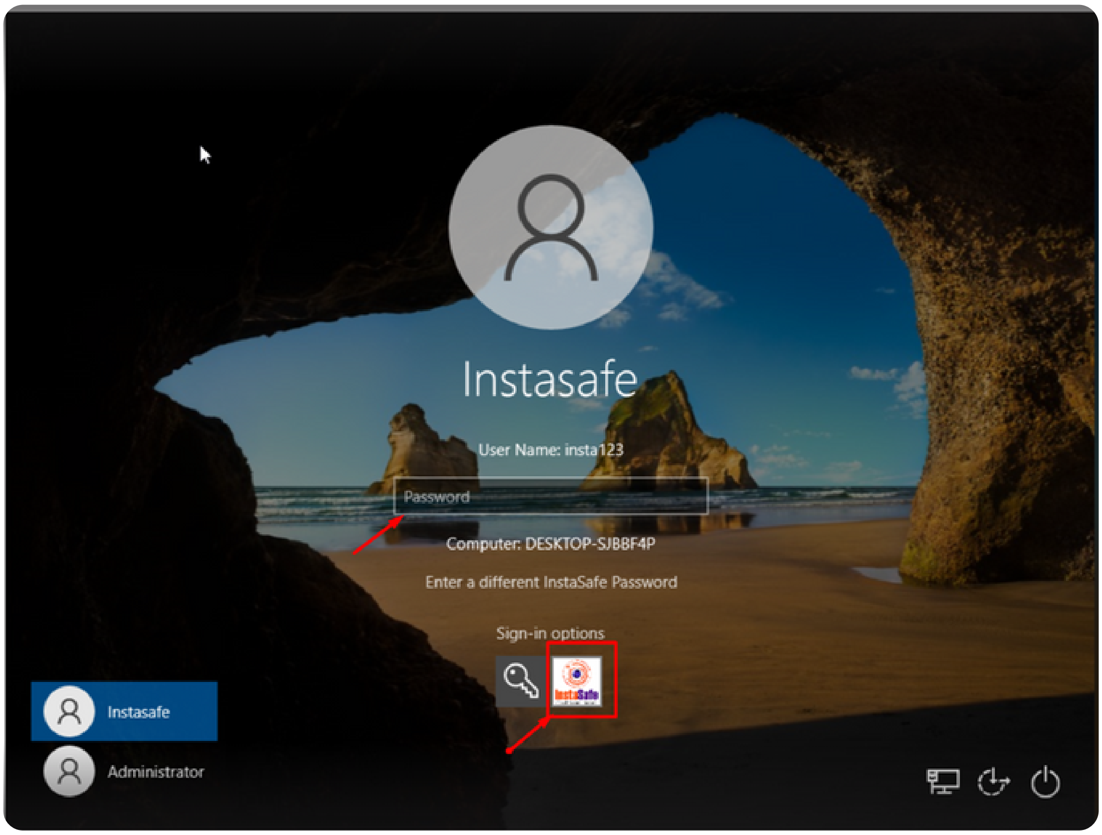
Enter a different InstaSafe Password

Sign-in options

Instasafe

Administrator

4. The user must select the InstaSafe icon



Instasafe

User Name: insta123

Password

Computer: DESKTOP-SJBBF4P

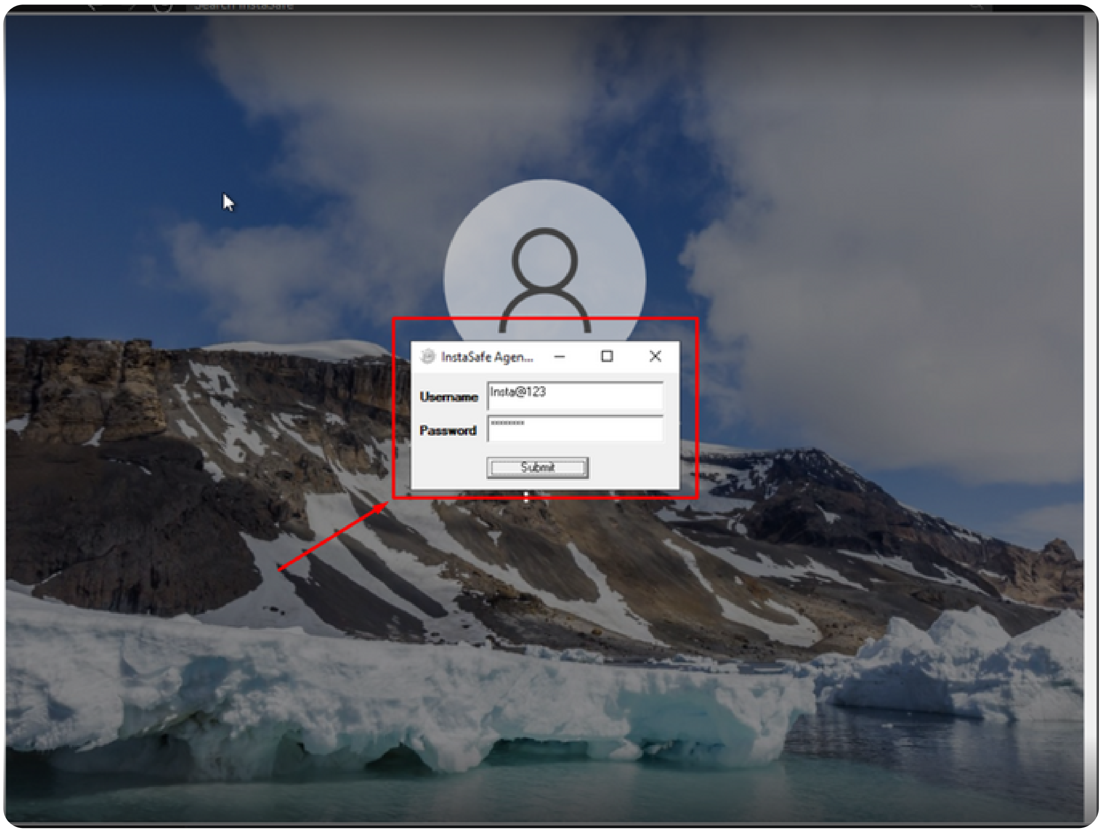
Enter a different InstaSafe Password

Sign-in options

Instasafe

Administrator

5. Enter their own AD Username/Password



Username Insta@123

Password *********

Benefits of Windows Autopilot and Azure AD Join with Always ON VPN

The Windows Autopilot User-Driven Hybrid Azure AD Join with Always On VPN offers several benefits in terms of device deployment, management, and user experience

Streamlined Deployment Process:

- Efficiency: The user-driven hybrid Azure AD join simplifies the deployment process by allowing users to take an active role. This can lead to faster onboarding of new devices as users can participate in the setup.

Flexibility in Network Connectivity:

- VPN Integration: The inclusion of Always On VPN ensures that the device can connect securely to the corporate network, even during the initial setup. This is especially advantageous for remote or mobile users who may not always be on-site.

Overcoming Network Challenges:

- VPN Validation Bypass: The ability to skip the Active Directory (AD) connectivity check when setting up Autopilot profiles helps overcome challenges associated with connecting to Windows Server AD through a VPN during the initial stages of device provisioning.

Improved User Experience:

- Continuity: Users experience a seamless transition during the Autopilot setup, as they can sign in directly to Windows Server AD from the logon screen. This enhances the overall user experience and reduces the likelihood of disruptions during the deployment process.

Reduced IT Intervention:

- Automation: By leveraging the user-driven approach and Always On VPN, IT intervention is minimized. Devices can progress through the setup process without requiring constant oversight, allowing IT teams to focus on more strategic tasks.

Enhanced Security:

- Secure Connectivity: The inclusion of Always On VPN ensures that the device connects securely to the corporate network, maintaining a higher level of security during the Autopilot setup and subsequent use.

Consistent Configuration:

- Enrollment Status Page: The Mobile Device Management (MDM) Enrollment Status Page (ESP) provides a clear view of configuration progress, including app and certificate installations. This transparency ensures that configurations are consistent and successful.

Adaptability to Various VPN Configurations:

- VPN Options: The flexibility to install different VPN clients or configure other settings necessary for VPN connectivity caters to the diverse requirements of organizations. This adaptability ensures that the solution can be tailored to specific network configurations.

In summary, the combination of Windows Autopilot User-Driven Hybrid Azure AD Join with Always On VPN offers a more user-friendly, flexible, and secure approach to deploying and managing Windows 10 devices in various network environments.

About InstaSafe

InstaSafe's mission is to secure enterprises from the abuse of excessive trust and privilege access. We empower organizations across to globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. Recognized by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access, InstaSafe Zero Trust Application Access, and InstaSafe Authenticator follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

Problems? Talk to us

Let's talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.

✉ sales@instasafe.com

🌐 www.instasafe.com

You can connect us at:

in /instasafe

f /instasafe

X /instasafe

▶ /instasafeZT