

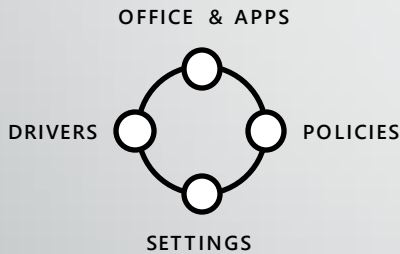


# Windows Autopilot

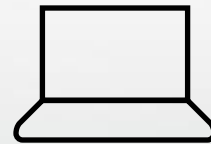
With INTUNE

# Why Autopilot?

- Traditional Windows deployment // The old way



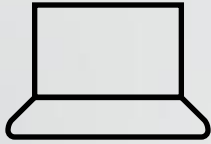
Build a custom image,  
gathering everything else  
that's necessary to deploy



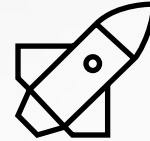
Time means money, making  
this an expensive  
preposition

# Why Autopilot?

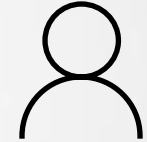
- Modern Windows deployment // **The new way**



Un-box and turn on  
off-the-shelf Windows PC



Transform with minimal  
user interaction



Device is ready  
for productive use

- Smart Device – knows who you are. A Zero Touch Experience for the end user.
- Reduces the burden on IT dept. , which in turn reduces the overall cost of provisioning the devices.
- Integration of M365 is much smoother. No need to build the custom images.

# Windows Autopilot Pre-requisites:-

Windows 10 version 1703 or higher

- Specific capabilities require higher versions

One of the following, to provide needed Azure Active Directory (automatic MDM enrollment and company branding features) and MDM functionality:

- Microsoft 365 Business subscriptions
- Microsoft 365 F1 subscriptions
- Microsoft 365 Enterprise E3 or E5 subscriptions, which include all Windows 10, Office 365, and EM+S features (Azure AD and Intune)
- Enterprise Mobility + Security E3 or E5 subscriptions, which include all needed Azure AD and Intune features
- Azure Active Directory Premium P1 or P2 (for auto enrollment).

# Windows Autopilot Pre-requisites:- (One time configurations)

## Azure Active Directory

- Configure automatic MDM enrollment.
- Configure company branding.
- Ensure users can join devices to Azure AD (for user-driven mode)

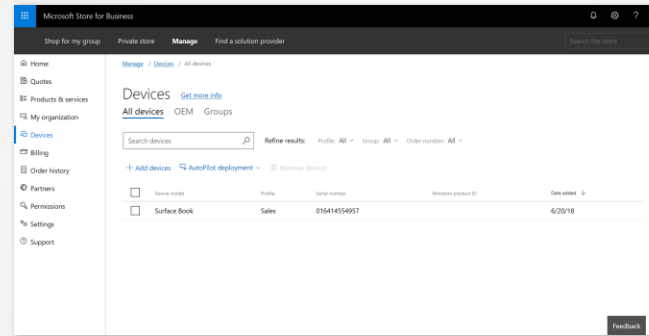
## Intune:

- Enable the enrollment status page (default ESP is already assigned to all users and all devices).
- Ensure users can enroll devices in Intune

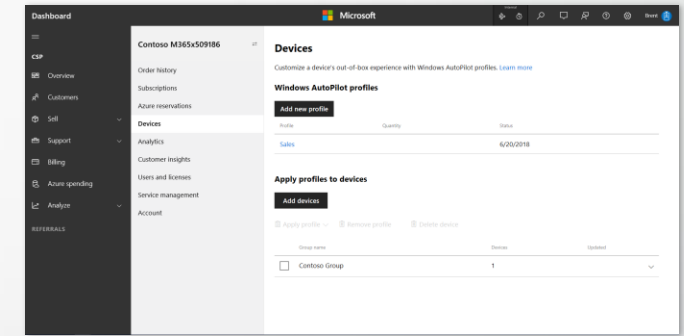
# Windows Autopilot Pre-requisites:- (Network Pre-reqs)

- <https://go.microsoft.com>
- <https://login.microsoftonline.com>
- <https://login.live.com>
- <https://account.live.com>
- <https://signup.live.com>
- <https://licensing.mp.microsoft.com>
- <https://licensing.md.mp.microsoft.com>
- <https://download.windowsupdate.com>

# Administering Windows Autopilot-

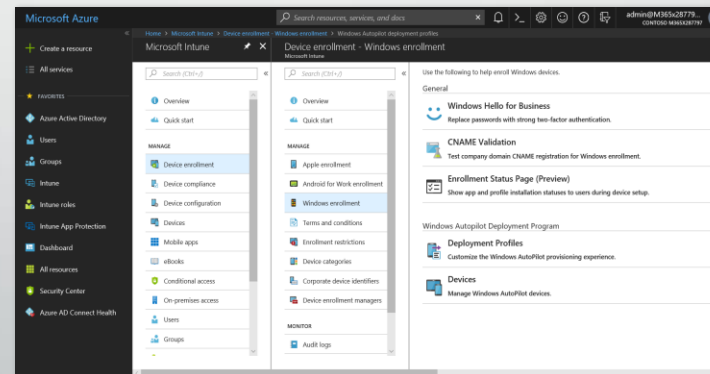


Microsoft Store for Business



Partner Center

The only  
portal  
enterprises  
should use



Microsoft Intune

# Autopilot Overview:-



```
graph TD; A[Autopilot Overview:-] --> B[Intune side]; A --> C[Device side];
```

## • Intune side

- Registering new devices – by OEM's or IT (uploading the HWID).
- AP devices gets the Azure AD object id's and they were added in security device groups.
- Configuration of Autopilot Deployment Profile and its assignation on the targeted device group.
- (Optional): Configuration of the ESP page. Windows 10, version 1803.

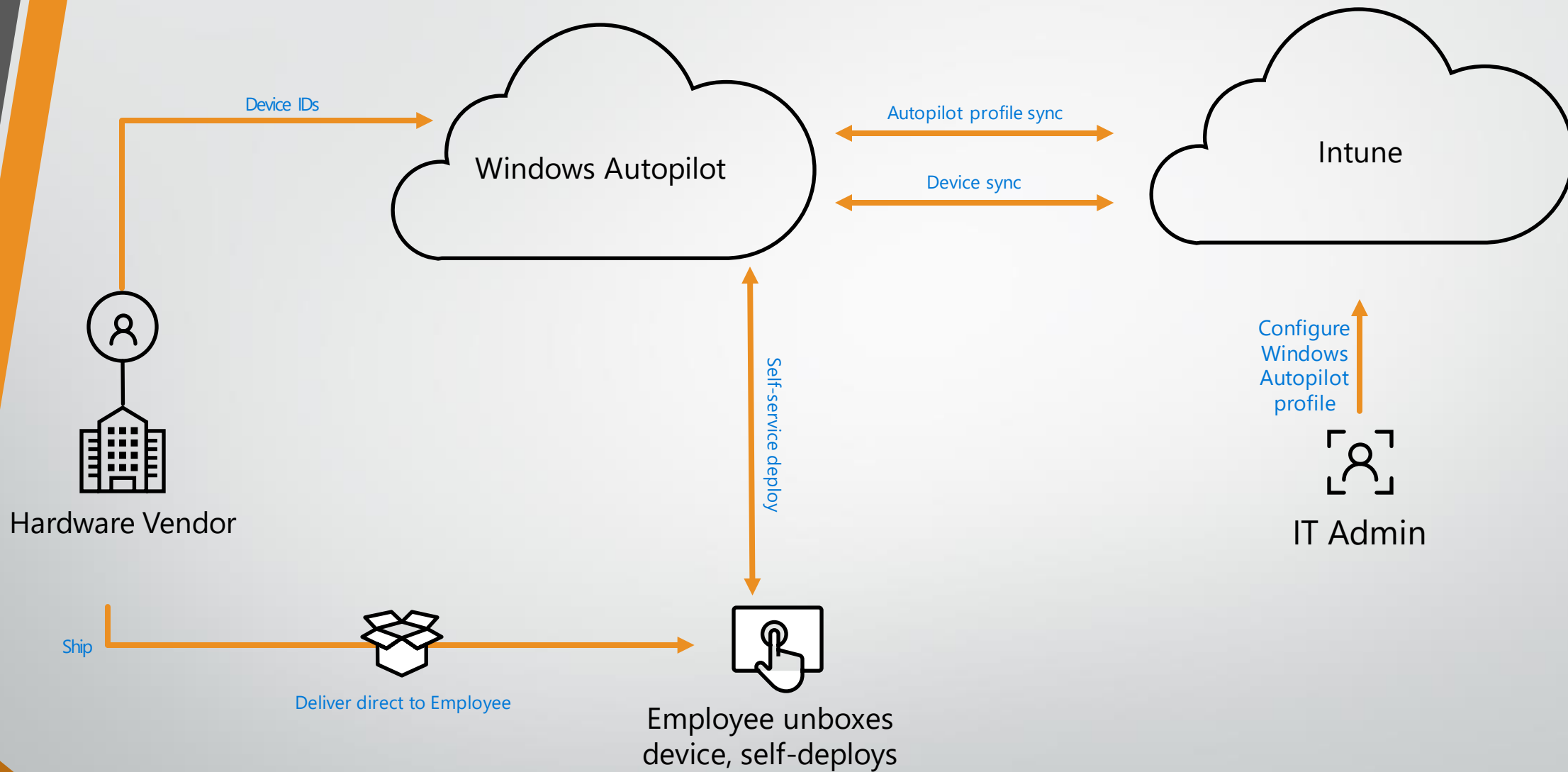
## • Device side

- Device shipped directly to the end user.
- User powers on the device.
- Choose the language, region and keyboard.
- Connect to a network.(if not wired)
- Azure AD authentication using custom branding.
- Azure AD registration and MDM enrollment happens.
- Device configuration policy will flow down + App deployment will take place.



# The Standard flow

- Once connected to a network, the device will download a Windows Autopilot profile specifying the settings that should be used (e.g. the prompts during OOBЕ that should be suppressed).
- Windows 10 will check for critical OOBЕ updates, and if any are available they will be automatically installed (rebooting if required).
- The user will be prompted for Azure Active Directory credentials, with a customized user experience showing the Azure AD tenant name, logo, and sign-in text.
- The device will join Azure Active Directory or Active Directory, based on the Windows Autopilot profile settings.
- The device will enroll in Intune (or other configured MDM services). (This occurs as part of the Azure Active Directory join process via MDM auto-enrollment, or before the Active Directory join process, as needed.)
- If configured, the [enrollment status page](#) (ESP) will be displayed.
- Once the device configuration tasks have completed, the user will be signed into Windows 10 using the credentials they previously provided. (Note that if the device reboots during the device ESP process, the user will need to re-enter their credentials as these are not persisted across reboots.)
- Once signed in, the enrollment status page will again be displayed for user-targeted configuration tasks.



# Continue in selected language?

English (United States)

Deutsch

suomi

français

norsk bokmål

русский

svenska

Let's start with region. Is this right?

U.S. Minor Outlying Islands

U.S. Virgin Islands

Uganda

Ukraine

United Arab Emirates

United Kingdom

United States

Yes



Ok, don't let me hold you up. Just pick the one you want from the list.



# Is this the right keyboard layout?

If you also use another keyboard layout, you can add that next.

US

Canadian Multilingual Standard

English (India)

Irish


Scottish Gaelic

United Kingdom

United States-Dvorak

Yes

After those 3 steps User authentication and further provisioning takes place

Account

# Hi Microsoft Support! Welcome to mod [redacted]

Let's get started. Enter your password for [redacted]


[Forgot password?](#)

[Need help?](#)

[Login to \[redacted\] orks](#)

Next

## MFA for added security:-



✕

# Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

### Step 1: How should we contact you?

Authentication phone

Select your country or region

Method

☒ Send me a code by text message

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2020 Microsoft

Legal

Privacy

Windows Security



## Set up a PIN

Create a PIN to use in place of passwords. Having a PIN makes it easier to sign in to your device, apps, and services.



☐ Include letters and symbols

OK

Cancel



# All set!

You can sign in with your PIN now.



OK

# Troubleshooting:-

- The first step should be to verify the Portal side configuration should be done correctly. This includes the AP device is successfully imported, added to the Windows AP devices and an Autopilot profile has a status- **"assigned"** on the device imported under Windows AP devices.
- Next step is to check the behavior and the kind of issue. Is the issue with all device or is it the just single device? Here we could narrow down to issue to a device specific if it is only one device. If all the devices experiencing the same issue, it must be a configuration or an issue with the device end like network proxy or the firewall, if all the Intune side configuration is correct.
- Common issues Admins usually experience is the machine is not undergoing to the Autopilot provisioning or an error code will be displayed straightaway on the OOB screen.

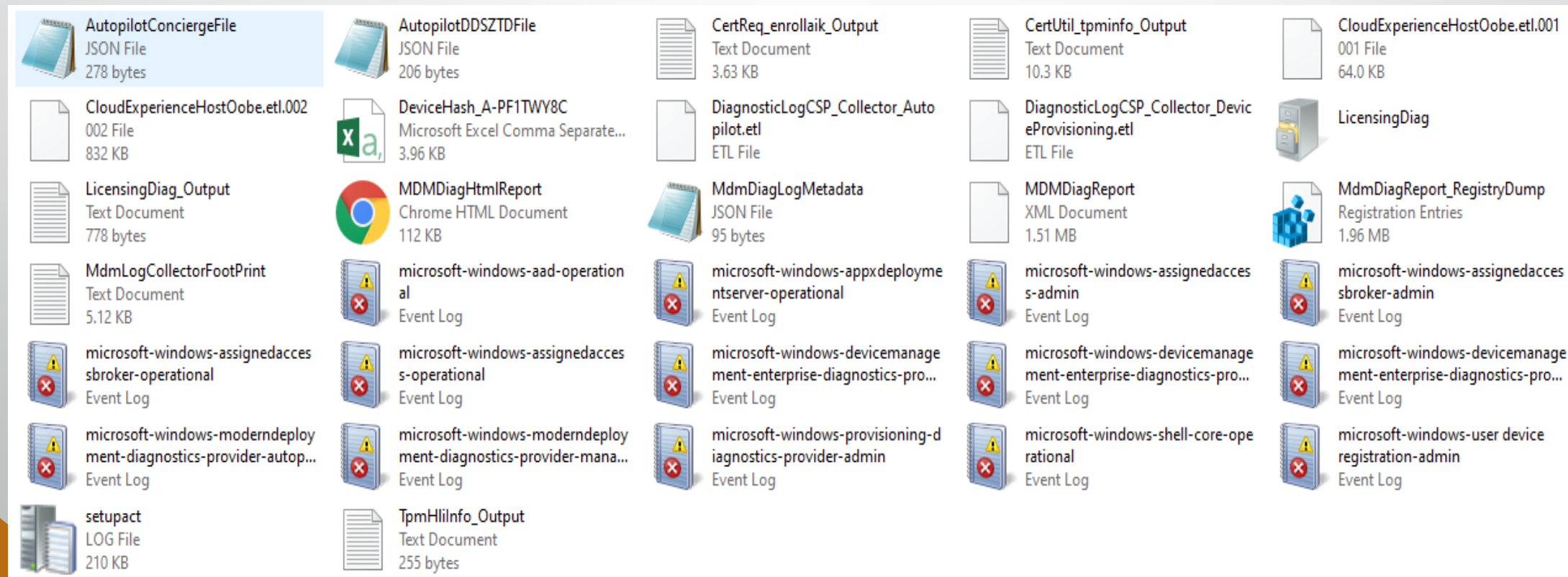
For the issue like device failed to provisioned and showing the normal OOB screen where it is asking for you to enter your windows account:-

- Ensure DNS name resolution for internet DNS names
- Allow access to all hosts via port 80 (HTTP), 443 (HTTPS), and 123 (UDP/NTP)
- **Windows Autopilot Deployment Service** - With Windows 10 version 1903 and above, the following URLs are used:  
<https://ztd.dds.microsoft.com>, <https://cs.dds.microsoft.com>

- Windows Activation- 0x8004FE33, Azure Active Directory- UPN validation, Network Time Protocol (NTP) Sync UDP port 123, Office 365 (IP ranges and Url's), Network Connection Status Indicator (NCI)- [www.msftconnecttest.com](http://www.msftconnecttest.com) must be resolvable via DNS and accessible via HTTP.

Places to consider for troubleshooting:-

- Autopilot CAB file: **MDMDiagnosticsTool.exe -area Autopilot -cab c:\Autopilot.cab**  
**MDMDiagnosticsTool.exe -area Autopilot;TPM -cab c:\autopilot.cab** – for self driven and whiteglove



<b>AutopilotDDSZTDFile.json</b>	<b>High</b>	This file contains the Autopilot profile settings being used for the device.
<b>DeviceHash_*.csv</b>	<b>High</b>	This contains the serial number and full hardware hash for the device. While that hash might not look useful to you, it tells us a lot about the device, including the version of Windows 10, patches that are installed, TPM firmware version, and a lot more stuff.
<b>IntuneManagementExtension.log</b>	<b>High</b>	This log will capture excruciating detail about the installation of Win32 apps being deployed via Intune. (Use one of the ConfigMgr log viewing tools, e.g. CMTrace.exe, to view this.)
<b>microsoft-windows-aad-operational.evtx</b>	<b>High</b>	This event log shows Azure AD join and Hybrid Azure AD Join-related info.
<b>microsoft-windows-devicemanagement-enterprise-diagnostics-provider-admin.evtx</b>	<b>High</b>	This event log covers MDM enrollment (including failure reasons) and other pertinent MDM activities.
<b>TpmHllInfo_Output.txt</b>	<b>High</b>	This log (which is created even when not specifying the TPM area) contains basic details about the TPM in the device: the manufacturer, the firmware level of that TPM, whether it has a required EK cert, etc.
<b>MDMDiagReport.xml</b>	<b>Medium</b>	This is a machine-readable XML version of the HTML report above.
<b>MdmDiagReport_RegistryDump.reg</b>	<b>Medium</b>	This dump the contents of a variety of registry keys that are useful to determining the state of the machine, including MDM enrollment details, Autopilot details, and related info. Support technicians may use this to find related information in Intune.

- Eventviewer Logs location-

***Application and Services Logs → Microsoft → Windows → Provisioning-Diagnostics-Provider → AutoPilot for versions before 1903, or Application and Services Logs → Microsoft → Windows → ModernDeployment-Diagnostics-Provider → AutoPilot for 1903 and above***

First, look at the AutopilotDDSZTDFile.json and check these settings:

- CloudAssignedDomainJoinMethod. If this is 0, the device has been configured to join Azure AD. If it is 1, the device has been configured to join AD (ODJ, Hybrid Azure AD Join).
- DeploymentProfileName. This will tell you the name of the Autopilot profile that was assigned to this device.
- CloudAssignedOobeConfig. This is a set of flags that specify how OOBЕ should behave (e.g. which pages should be skipped). For user-driven scenarios, you'll typically see a value of 28 (user should not be an admin) or 30 (user should be an admin) although that could change as new settings are added.

```
{ "AutopilotServiceCorrelationId": "cc9f37d2-e7dd-4837-985b-d7c47",  
  "ZtdRegistrationId": "a588b978-04cf-4221-b146-ce0fc46be6c7",  
  "AadDeviceId": "08168089-556e-4d0c-8388-6a61c22a4b1d",  
  "CloudAssignedDomainJoinMethod": 0,  
  "CloudAssignedTenantDomain": "abhinavsengar786.onmicrosoft.com",  
  "DeploymentProfileName": "autopilot1",  
  "PolicyDownloadDate": "2020-04-20T19:55:15Z",  
  "CloudAssignedOobeConfig": 1290 }
```

- Registry Path: **HKLM\SOFTWARE\Microsoft\Provisioning\Diagnostics\AutoPilot**
- Advanced Network Analysis using Fiddler logs. At the OOB stage, press F10 and install the setup from external USB.
- Not to forget client side flow. 😊





# THANK YOU.

By – Abhinav Sengar