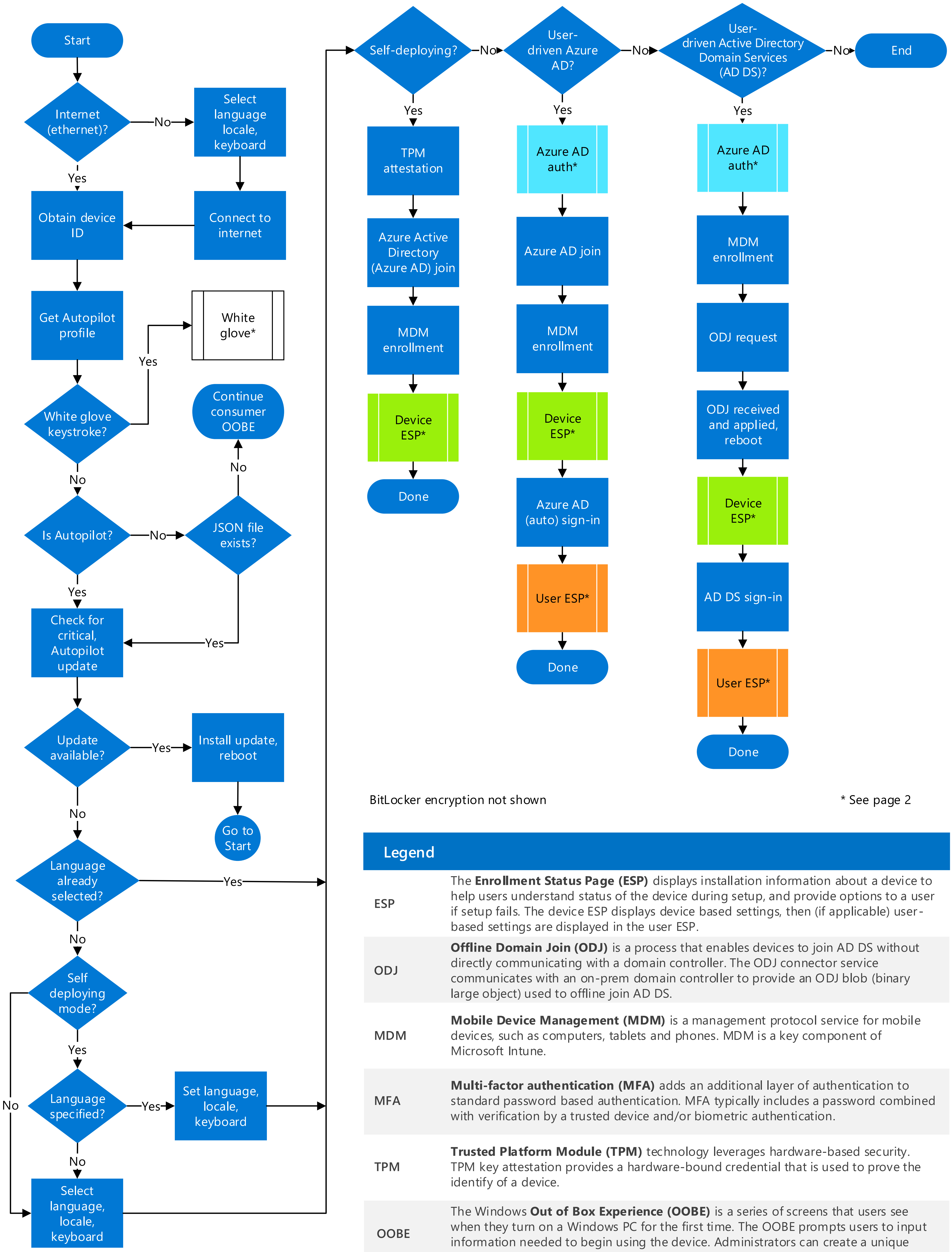
Windows 10 Autopilot deployment process



Start

Internet (ethernet)?

No → Select language locale, keyboard → Connect to internet → Obtain device ID

Yes → Obtain device ID

Get Autopilot profile

White glove keystroke?

Yes → White glove*

No → Is Autopilot?

No → JSON file exists?

No → Continue consumer OOBE

Yes → Check for critical, Autopilot update

Is Autopilot? Yes → Check for critical, Autopilot update

Update available?

Yes → Install update, reboot → Go to Start

No → Language already selected?

Yes → Self-deploying?

No → Self deploying mode?

Yes → Language specified?

Yes → Set language, locale, keyboard → Self-deploying?

No → Select language, locale, keyboard → Self-deploying?

Self deploying mode? No → Select language, locale, keyboard

Self-deploying?

Yes → TPM attestation → Azure Active Directory (Azure AD) join → MDM enrollment → Device ESP* → Done

No → User-driven Azure AD?

Yes → Azure AD auth* → Azure AD join → MDM enrollment → Device ESP* → Azure AD (auto) sign-in → User ESP* → Done

No → User-driven Active Directory Domain Services (AD DS)?

Yes → Azure AD auth* → MDM enrollment → ODJ request → ODJ received and applied, reboot → Device ESP* → AD DS sign-in → User ESP* → Done

No → End

BitLocker encryption not shown

* See page 2

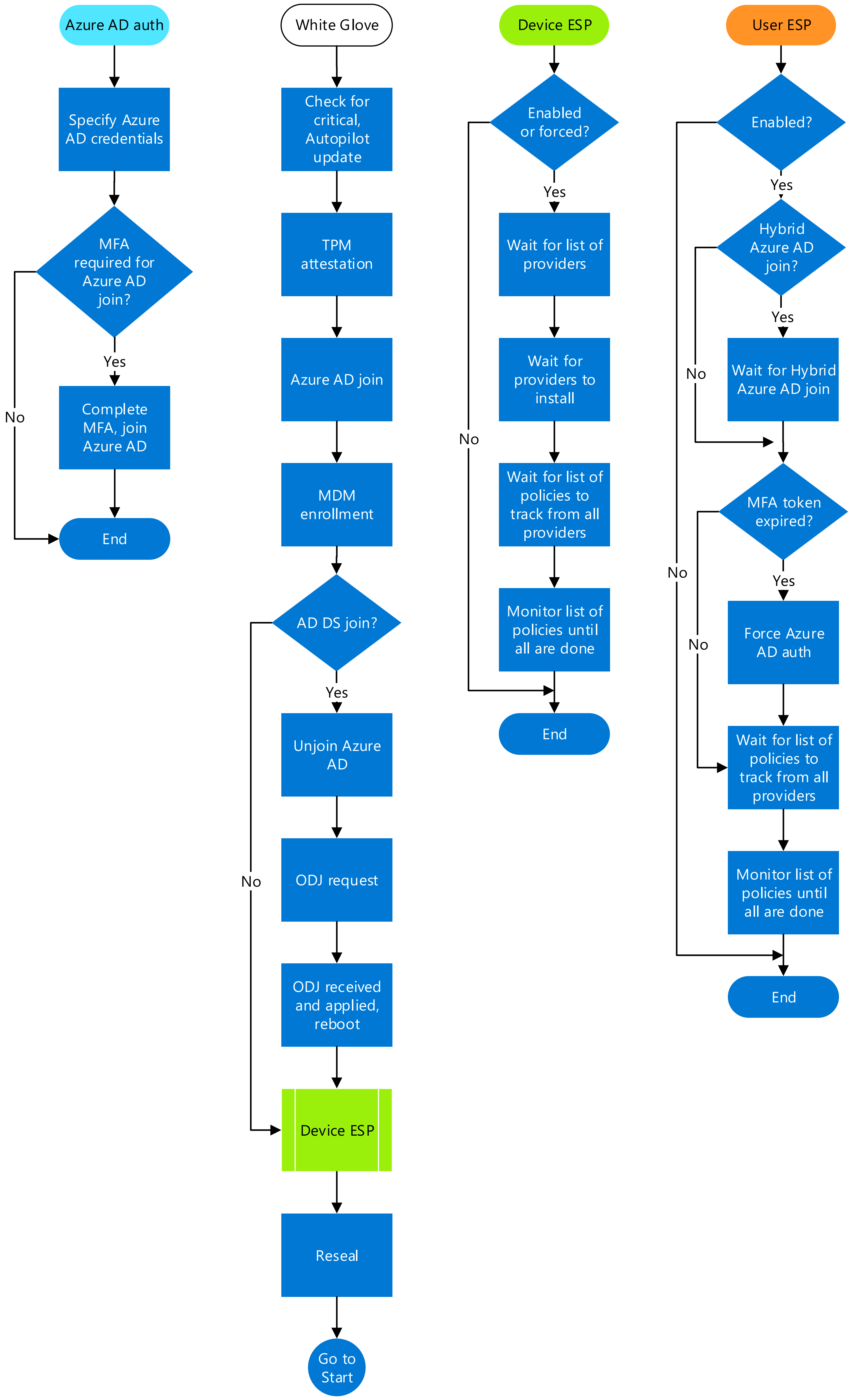
Legend

ESP	The **Enrollment Status Page (ESP)** displays installation information about a device to help users understand status of the device during setup, and provide options to a user if setup fails. The device ESP displays device based settings, then (if applicable) user-based settings are displayed in the user ESP.
ODJ	**Offline Domain Join (ODJ)** is a process that enables devices to join AD DS without directly communicating with a domain controller. The ODJ connector service communicates with an on-prem domain controller to provide an ODJ blob (binary large object) used to offline join AD DS.
MDM	**Mobile Device Management (MDM)** is a management protocol service for mobile devices, such as computers, tablets and phones. MDM is a key component of Microsoft Intune.
MFA	**Multi-factor authentication (MFA)** adds an additional layer of authentication to standard password based authentication. MFA typically includes a password combined with verification by a trusted device and/or biometric authentication.
TPM	**Trusted Platform Module (TPM)** technology leverages hardware-based security. TPM key attestation provides a hardware-bound credential that is used to prove the identify of a device.
OOBE	The Windows **Out of Box Experience (OOBE)** is a series of screens that users see when they turn on a Windows PC for the first time. The OOBE prompts users to input information needed to begin using the device. Administrators can create a unique Autopilot OOBE by configuring an Autopilot profile for a device.

October 2019

Microsoft

Windows 10 Autopilot deployment process


Azure AD auth
Specify Azure AD credentials
MFA required for Azure AD join?
Yes
No
Complete MFA, join Azure AD
End
White Glove
Check for critical, Autopilot update
TPM attestation
Azure AD join
MDM enrollment
AD DS join?
Yes
No
Unjoin Azure AD
ODJ request
ODJ received and applied, reboot
Device ESP
Reseal
Go to Start
Device ESP
Enabled or forced?
Yes
No
Wait for list of providers
Wait for providers to install
Wait for list of policies to track from all providers
Monitor list of policies until all are done
End
User ESP
Enabled?
Yes
No
Hybrid Azure AD join?
Yes
No
Wait for Hybrid Azure AD join
MFA token expired?
Yes
No
Force Azure AD auth
Wait for list of policies to track from all providers
Monitor list of policies until all are done
End