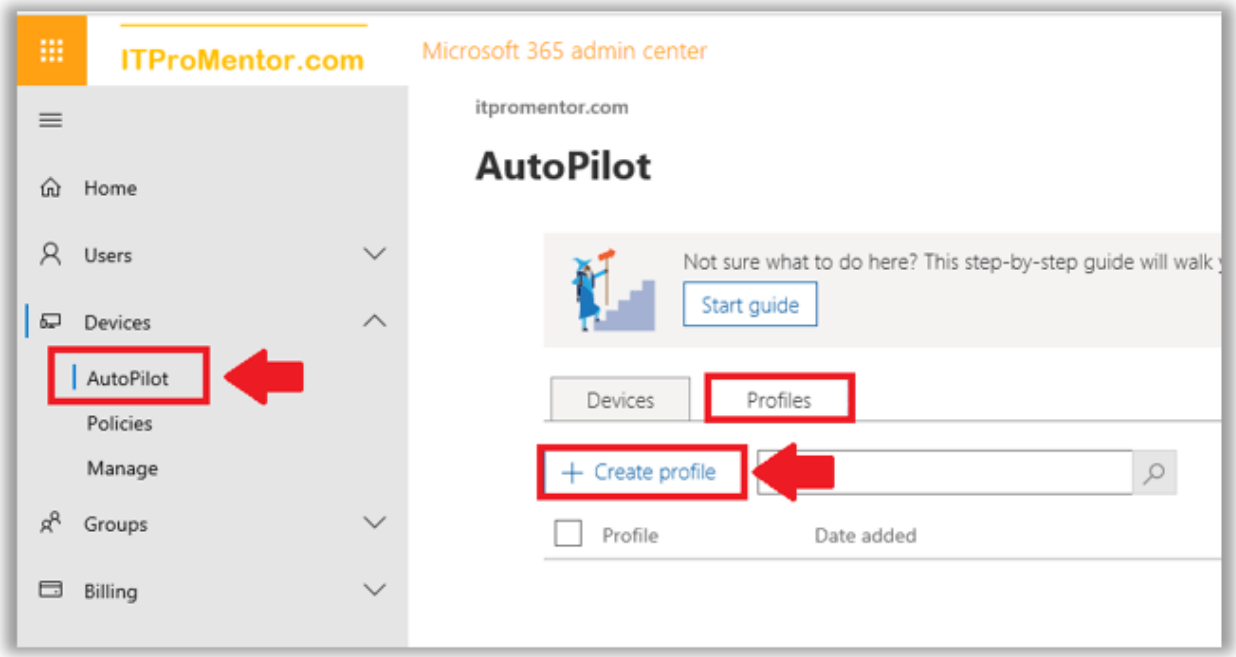
What are the benefits of using Autopilot in Microsoft 365? And, how to configure it.

by Alex 21. February 2019 Technical 1



Autopilot is a “low touch” or “no touch” deployment method that can be leveraged by IT departments to enable self-service computer deployments. Users can basically pick up a new Windows 10 device, sign in, and have all of their applications and data come to them (no profile migration, etc. required).

But its actual capabilities and benefits are a little bit oversold, I think. Even before Autopilot was available, using Intune you could automate the deployment of applications to Azure AD joined (and MDM enrolled) machines. The “Autopilot” piece that is configurable via the 365 admin center and stapled on top of Intune, again, is just icing on the cake.

But, if you can get it all dialed in with a process down pat–Autopilot still has some benefits worth considering.

Let me just be clear on what the user experience could be like, even without enabling the “Autopilot” feature and pre-enrolling all your hardware in the portal.

- Users can self-join their Windows 10 devices to Azure AD using the Out-of-box-experience (OOBE)
- Joined devices will also become auto-enrolled in Intune (and this is possible by default using any Microsoft 365 plan for which you have completed the initial wizard-driven configurations)
- If you selected the option during initial setup wizards, their Office applications will also be deployed to them automatically
- Other third-party applications can be deployed over the air also, just using Intune (you just need to take the time to set that up in your tenant)

So before you even get to the Autopilot configuration, you can accomplish quite a lot that cuts down on deployment time. So why would you want to go through the extra hassle of getting it setup?

Here are the deltas–the real benefits of using this service:

- Users can have a “branded” OOBE, rather than the default experience–probably not a huge deal to many small orgs out there
- By pre-registering the device ID’s to your tenancy, it would not be possible for that device to even accidentally join another organization

- If you operate in a hybrid environment, you as an admin can control whether the devices will become Azure AD Joined only, or Hybrid Azure AD Joined with the local AD also (by default when you self-join/enroll with Azure AD and Intune your device will be Azure AD joined only)*
- As an admin, you can also control whether or not the user will be made a local administrator on the machine (which is again the default behavior out of the box)

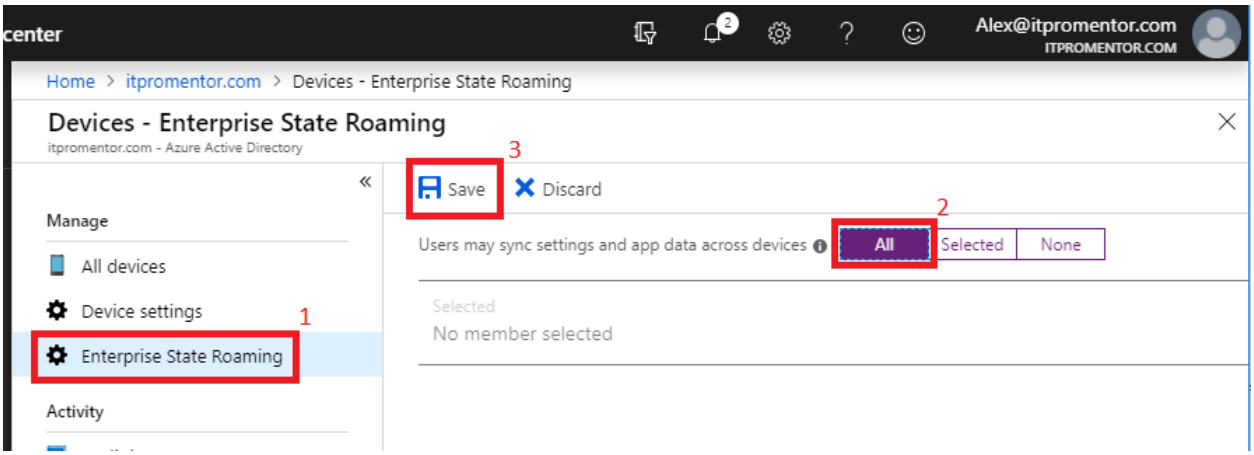
I think it is that last one that is more important than the others. Even the hybrid join option probably will not matter much to small organizations who are unloading more and more premises-based dependencies. After all, it is possible for an Azure AD joined machine (participating in a properly configured hybrid environment with Azure AD Connect) to access local domain resources via SSO, without actually joining the domain.

**This requires some extra configuration and an on-premises Intune connector service*

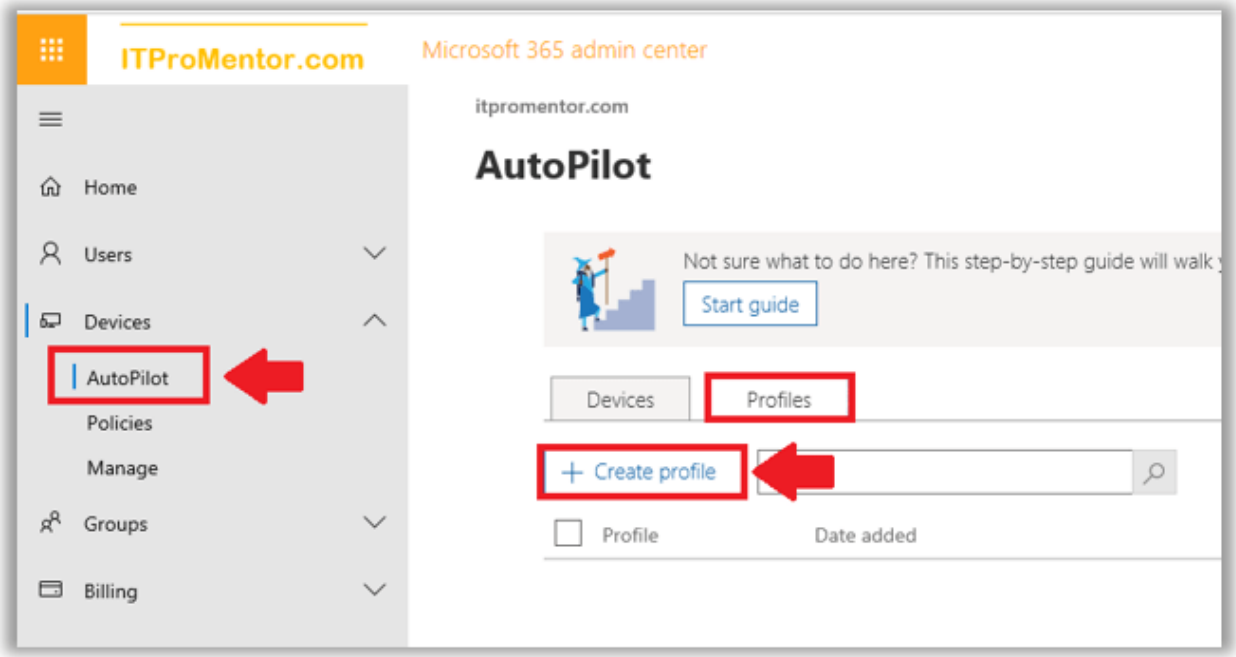
How to use Autopilot in Microsoft 365

Just a quick note, I am using the Business subscription in this demonstration, which is the lowest common denominator subscription available among the Microsoft 365 plans, and appropriate for many small and mid-sized orgs.

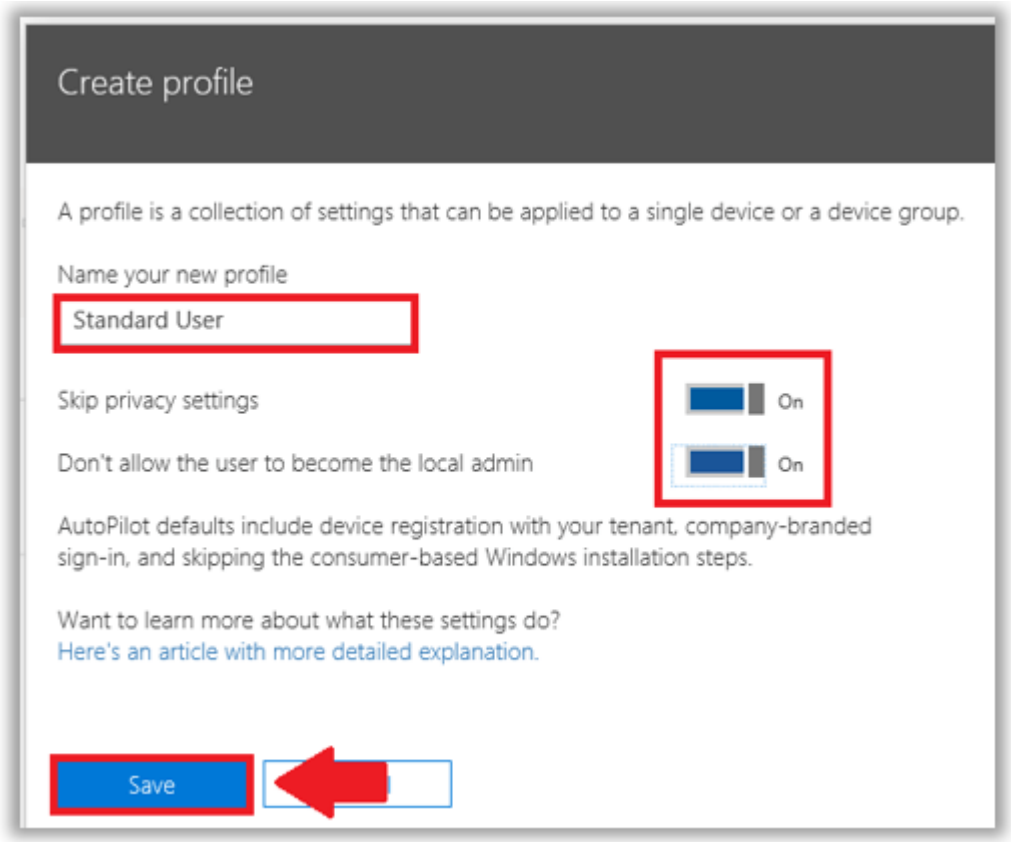
Before we start, it is recommended to also have Enterprise State Roaming configured. This allows a user's settings to sync between devices automatically.



Create an Autopilot profile from the Microsoft 365 admin portal. Navigate to **Devices > Autopilot**. Choose the **Profiles** tab and then **+ Create profile**.



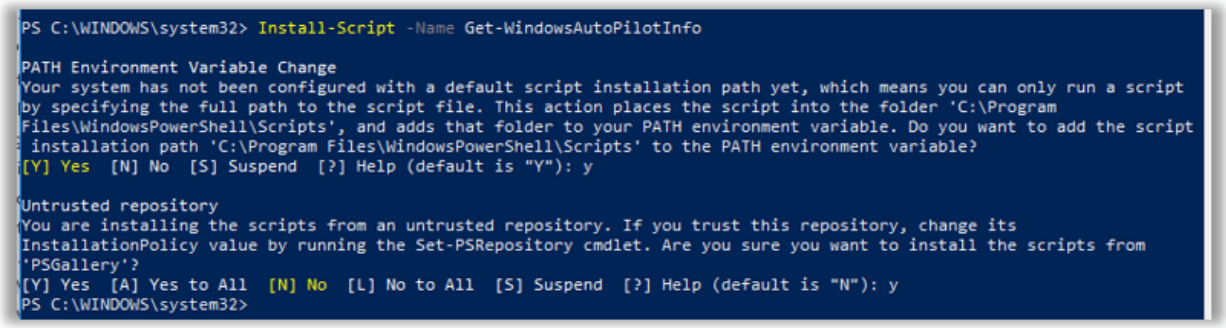
We don't have that many options, but they are the ones we want the most—**Skip privacy settings** and **Don't allow the user to become the local admin**. I recommend enabling both for most "Standard" user accounts, but you could also create an Admin User profile, for "super users" or other desktop admins.



Add Autopilot devices

It is possible to work with OEM's to get the necessary device ID information imported into Microsoft 365. Not everyone will have access to this yet, so you can get started using the manual method (meaning you still have to touch the individual workstations).

Install-Script -Name Get-WindowsAutoPilotInfo



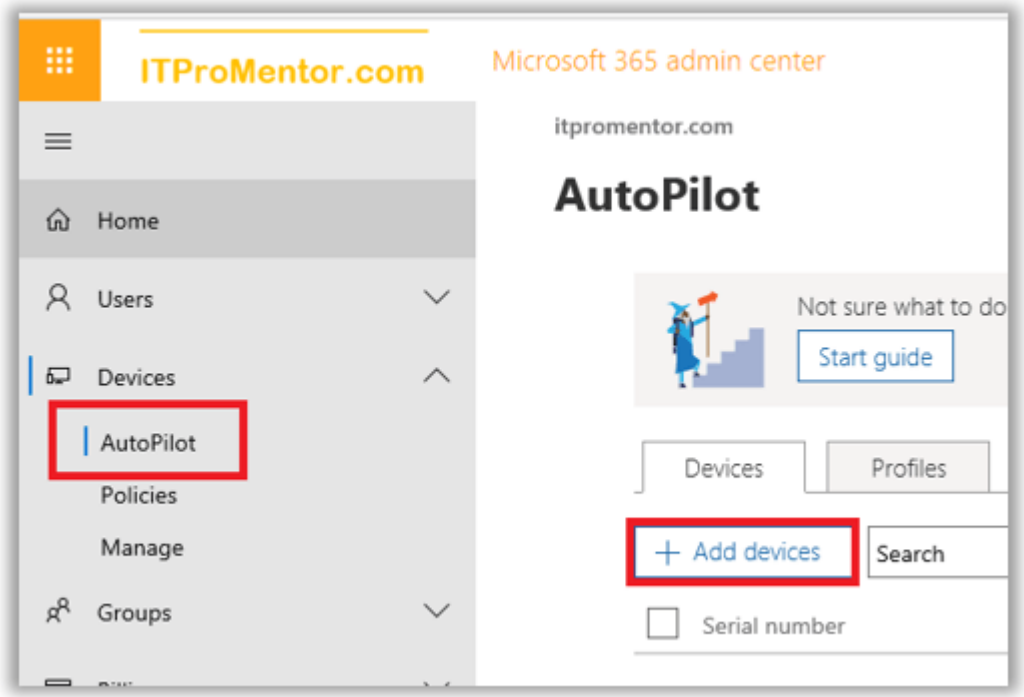
To run the script, first enable unrestricted execution policy:

Set-ExecutionPolicy unrestricted

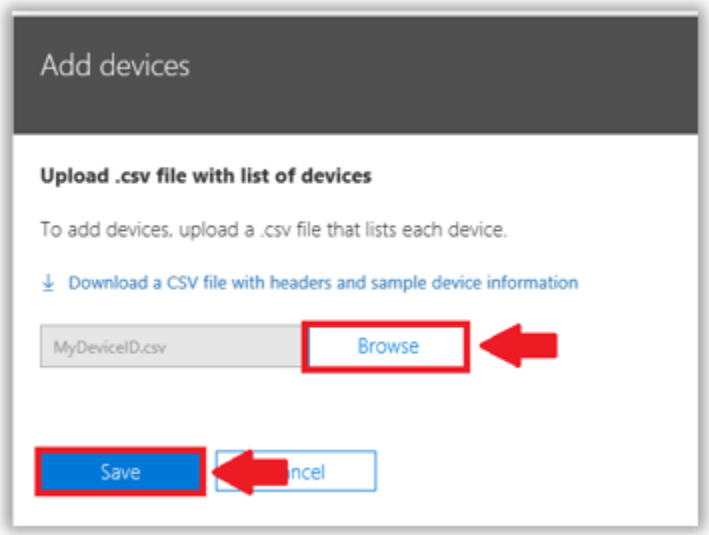
Finally, the command to execute the script is:

.\Get-WindowsAutoPilotInfo.ps1 -OutputFile .\MyDeviceID.csv

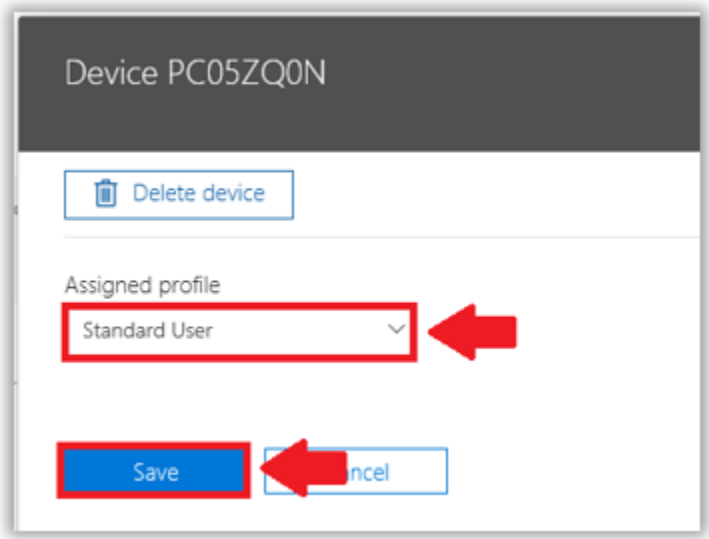
Once you have the csv file, you can upload this file into the Microsoft 365 Business admin portal. Go back to **Devices > Autopilot** and click on **+ Add devices**.



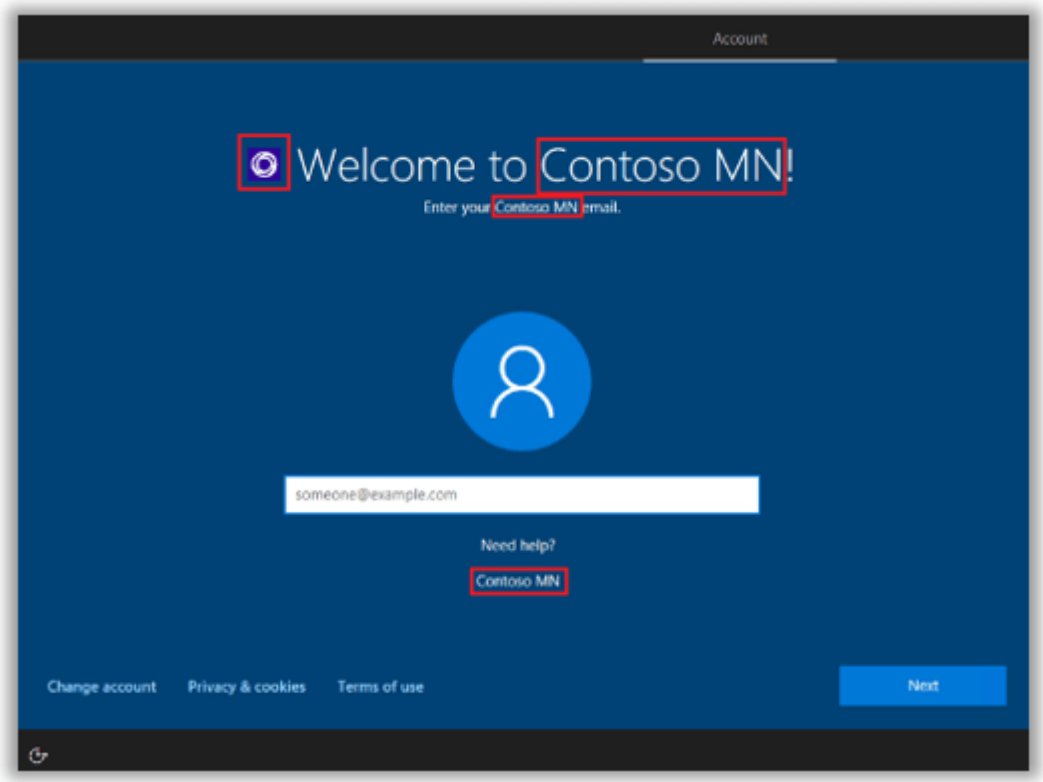
Browse to your csv file and upload it to the portal.



This can take some time to take effect, but once it is available, select your device and then assign your desired profile to it. **Save**.



The result of this work, is that when a user identifies themselves to the device as belonging to the organization (signing in with their work/school account), then Azure AD will recognize the device and give the user a “low-touch” deployment experience, joining the device to Azure AD and enrolling it with the Intune service for MDM in the process.



In case you need to do any troubleshooting with the enrollment process, check out this Microsoft TechNet article.

Windows 10 Autopilot: Hybrid-Join

As I mentioned, Autopilot was initially only possible for Azure-AD Joined devices (non-Hybrid). If you use the default method which is exposed via the Microsoft 365 admin center, then the device state of the local computer will be Azure AD-Joined at the end of the process.

However, using an on-premises Intune connector service, it is now possible to enable a Hybrid-Join experience with Windows 10 Autopilot. This feature is still in preview at the time of this writing, and is available only via the Intune portal (the option does not appear in the Microsoft 365 admin portal yet).

The major pre-requisites here are:

- You must already have Hybrid Join enabled and working via Azure AD Connect
- Elect a Windows Server 2016 server for the Intune connector service
- Delegate permissions to create computer objects to an Intune service account
- Autopilot devices must be on-site with the local Active Directory (VPN is not supported)

I am not going to cover this process—as I mentioned this feature is still in preview, and is targeted more at Enterprise environments with long-term hybrid coexistence needs. You may refer to the full article at Microsoft which describes the process in detail if it suits your needs. (But, I think a lot of small orgs might just skip this and start managing their devices via Azure AD / Intune, which removes yet another dependency from the local network.)