Lab 3A – Intune Autopilot & Active Directory Setup (with Evidence)

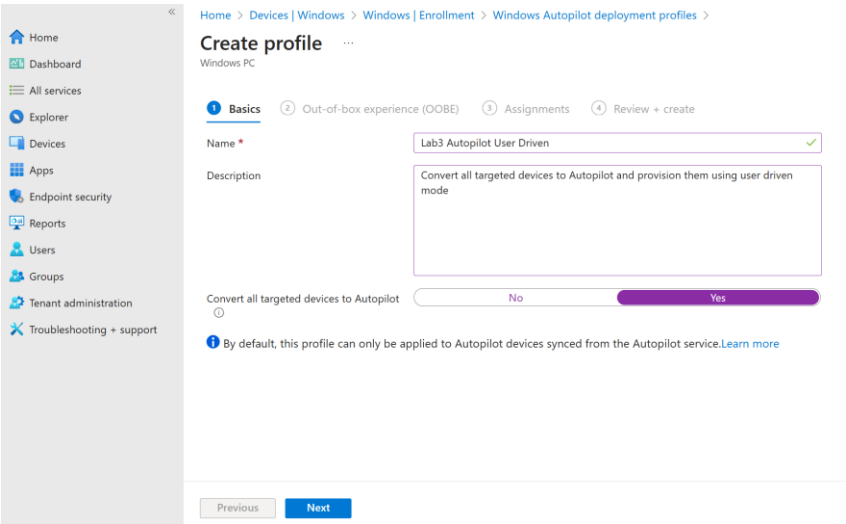
Lab 3 – Summary

In this lab, I created and configured a Windows Autopilot deployment profile to customize the out-of-box experience (OOBE) for Windows devices. The deployment profile ensures that when a user powers on a new or reassigned device, it is automatically provisioned and configured according to organizational standards.

- **Microsoft Entra ID** provided identity and access management, ensuring users authenticate securely.
- **Microsoft Intune** was used to push out policies, apps, and security settings.
- **Microsoft Endpoint Manager (MEM)** served as the admin console, allowing me to monitor compliance and manage devices.

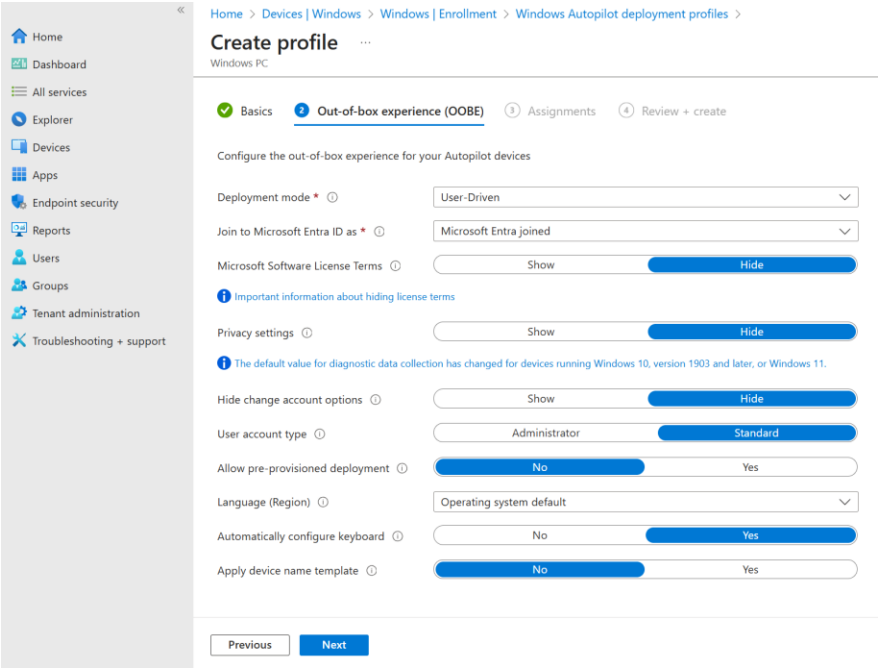
By combining these three components, Autopilot delivers a seamless user experience where devices are pre-configured with policies, identity controls, and applications during first boot, ensuring both security and productivity.

Step 1 – Basics



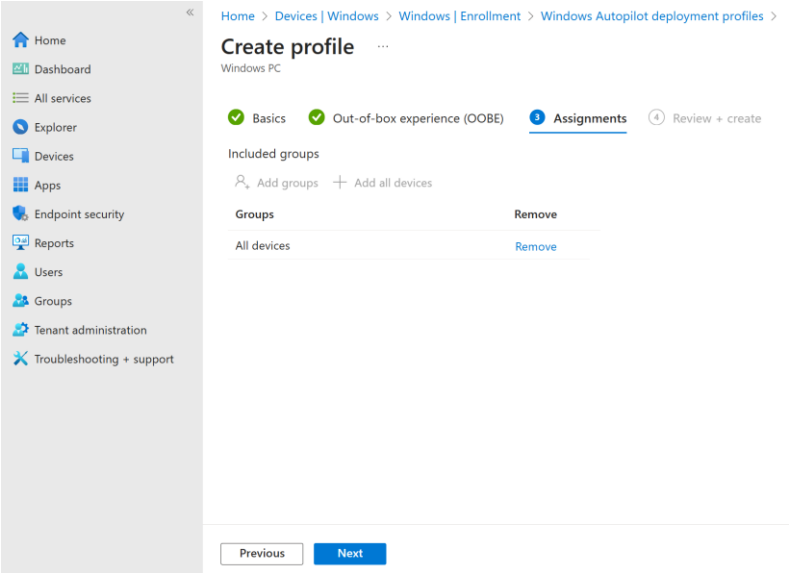
Notes: Named the profile *Lab3 – Autopilot User Driven*, described it as deploying Windows devices in user-driven mode, and enabled conversion so all targeted devices are automatically registered as Autopilot devices

Step 2 – Out-of-box experience (OOBE)



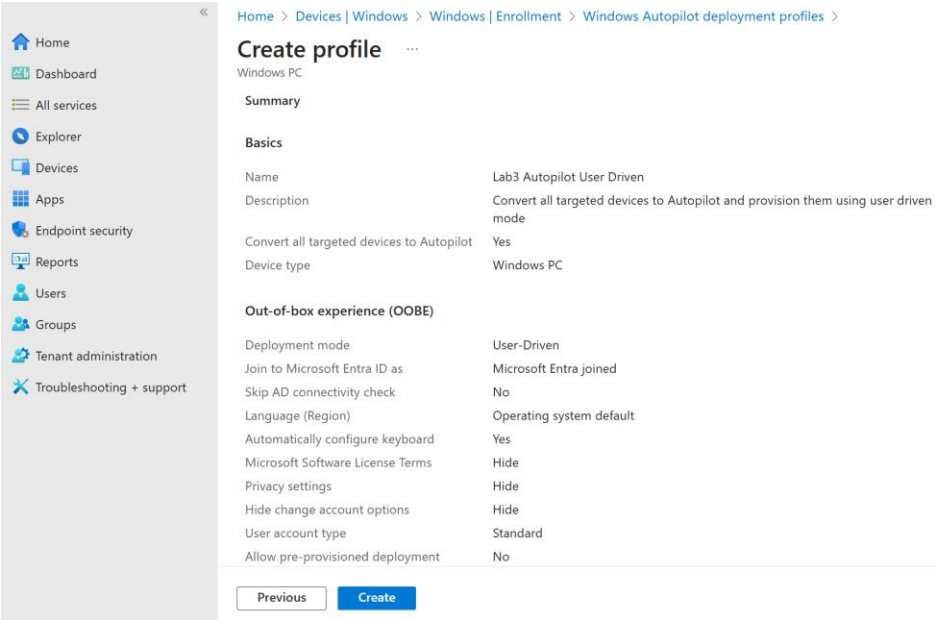
Notes: Configured OOBE for user-driven deployment with Microsoft Entra join, hidden license/privacy pages, hidden account options, and Standard User account type. This enforces least privilege while simplifying the user's setup process.

Step 3 – Assignments



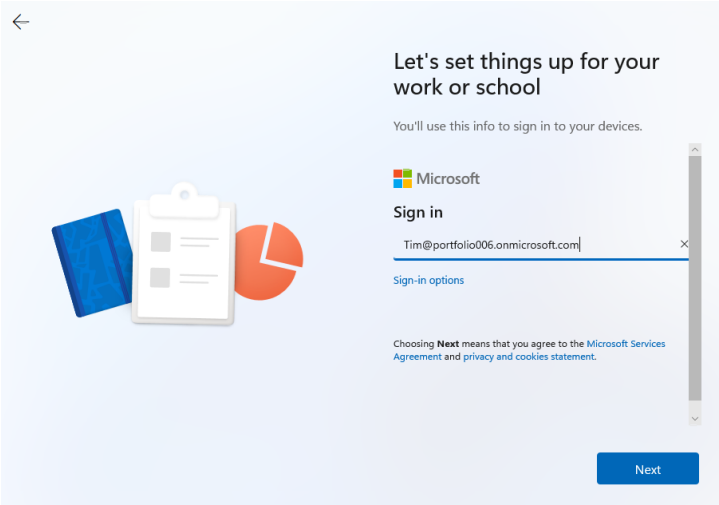
Notes: Assigned the Autopilot profile to all devices in the tenant, ensuring that any enrolled Windows device will receive the OOBE and policy settings

Step 4 – Review + Create

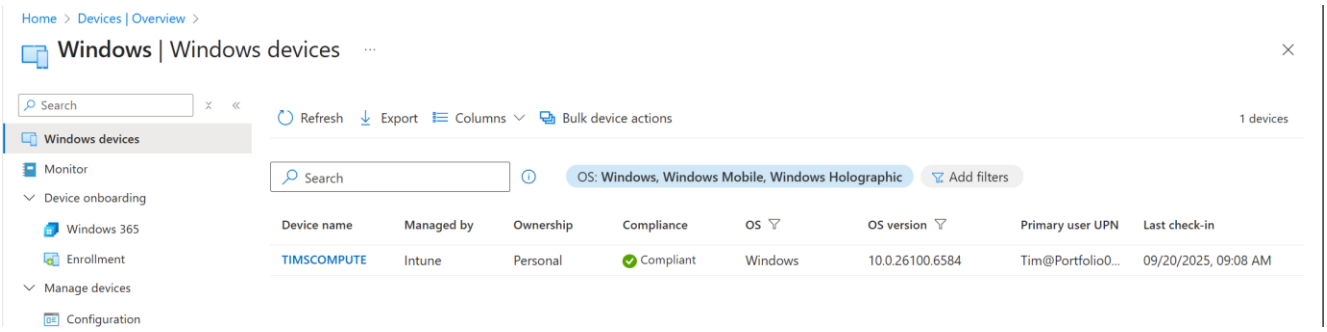


Notes: Reviewed all settings for the Autopilot deployment profile and confirmed creation. The profile is now ready to automatically provision devices with Entra ID join and Intune enrollment using user-driven deployment.

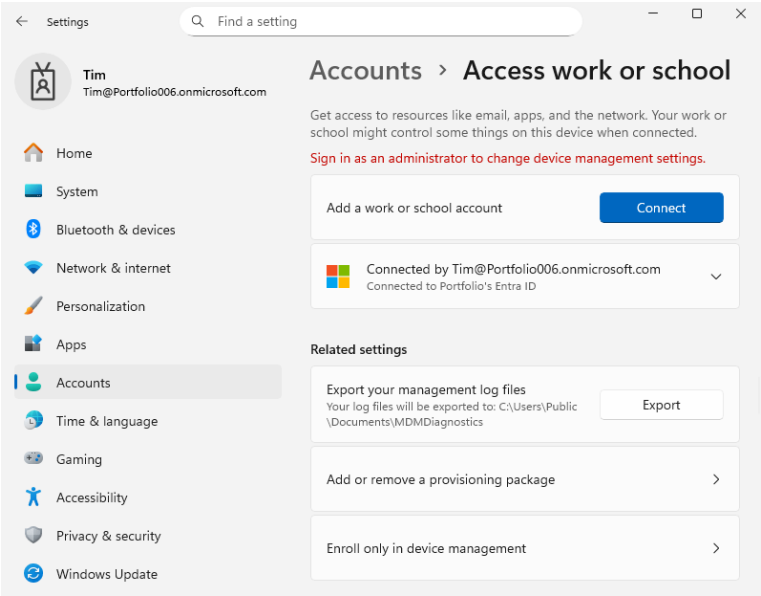
Part 2 – Test Autopilot with VM



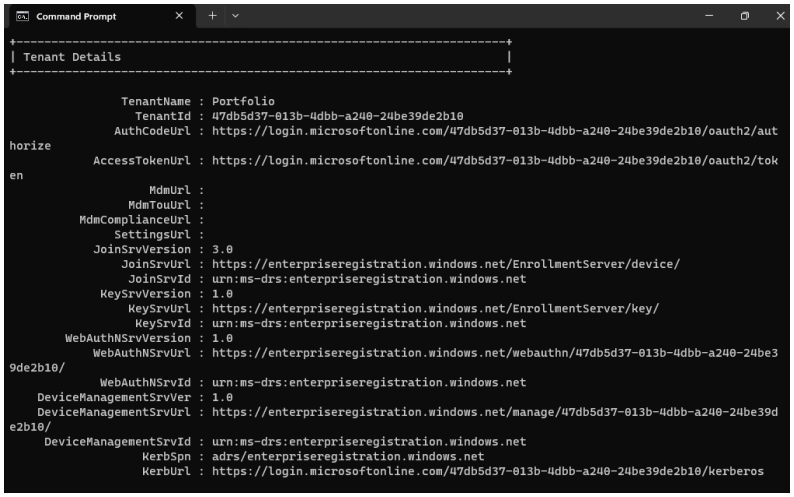
Notes: Signed in with Tim's Entra ID test account during OOBE, ensuring the VM connected to my Microsoft 365 tenant. Multi-Factor Authentication (MFA) was enforced as an added security step, and Windows Hello for Business prompted Tim to set a unique device PIN. This confirmed successful identity management and secure provisioning through Entra ID



Notes: Confirmed that Tim's VM enrolled successfully into Intune MDM. Device appears in Endpoint Manager as TIMSCOMPUTER, marked as Personal, Compliant, and managed by Intune. Last check-in shows recent timestamp, verifying ongoing policy sync



Notes: On Tim's VM, confirmed that device was connected to Entra ID but management settings were restricted, showing red warning text requiring administrator rights. This confirmed that Tim is a standard user under least privilege, while the device remained fully enrolled and compliant in Intune as seen from the Endpoint Manager portal



```
Command Prompt

+----------------------------------------------------------------------+
| Tenant Details                                                       |
+----------------------------------------------------------------------+

                TenantName : Portfolio
                  TenantId : 47db5d37-013b-4dbb-a240-24be39de2b10
                AuthCodeUrl : https://login.microsoftonline.com/47db5d37-013b-4dbb-a240-24be39de2b10/oauth2/aut
horize
             AccessTokenUrl : https://login.microsoftonline.com/47db5d37-013b-4dbb-a240-24be39de2b10/oauth2/tok
en
                     MdmUrl :
                  MdmTouUrl :
          MdmComplianceUrl :
                SettingsUrl :
            JoinSrvVersion : 3.0
                JoinSrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/device/
                 JoinSrvId : urn:ms-drs:enterpriseregistration.windows.net
             KeySrvVersion : 1.0
                 KeySrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/key/
                  KeySrvId : urn:ms-drs:enterpriseregistration.windows.net
        WebAuthNSrvVersion : 1.0
            WebAuthNSrvUrl : https://enterpriseregistration.windows.net/webauthn/47db5d37-013b-4dbb-a240-24be3
9de2b10/
             WebAuthNSrvId : urn:ms-drs:enterpriseregistration.windows.net
    DeviceManagementSrvVer : 1.0
    DeviceManagementSrvUrl : https://enterpriseregistration.windows.net/manage/47db5d37-013b-4dbb-a240-24be39d
e2b10/
     DeviceManagementSrvId : urn:ms-drs:enterpriseregistration.windows.net
                   KerbSpn : adrs/enterpriseregistration.windows.net
                   KerbUrl : https://login.microsoftonline.com/47db5d37-013b-4dbb-a240-24be39de2b10/kerberos
```

Notes: Ran dsregcmd /status on Tim's VM and confirmed the device was Azure AD joined (AzureAdJoined : YES). However, the MDM enrollment fields (MdmUrl, MdmUserUPN, MdmEnrollment) were blank. This occurs because Tim is a standard user without local administrator rights, which restricts visibility into device management details. From the Endpoint Manager portal, the device appears fully enrolled and compliant, showing that MDM enrollment succeeded — the blank fields on the local device simply reflect limited user permissions rather than a failed enrollment.

Lab 3A – Summary

Summary, in this lab I set up a Windows device with Autopilot, joined it to Microsoft Entra ID, and enrolled it into Intune MDM. I made sure users only had standard accounts, policies were applied at first boot, and MFA with Windows Hello for Business was in place for secure sign-ins.

This showed how Autopilot can make device setup easier while still keeping things secure. It also proved that role-based access works — users couldn't bypass restrictions, and compliance stayed managed through Endpoint Manager.