

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

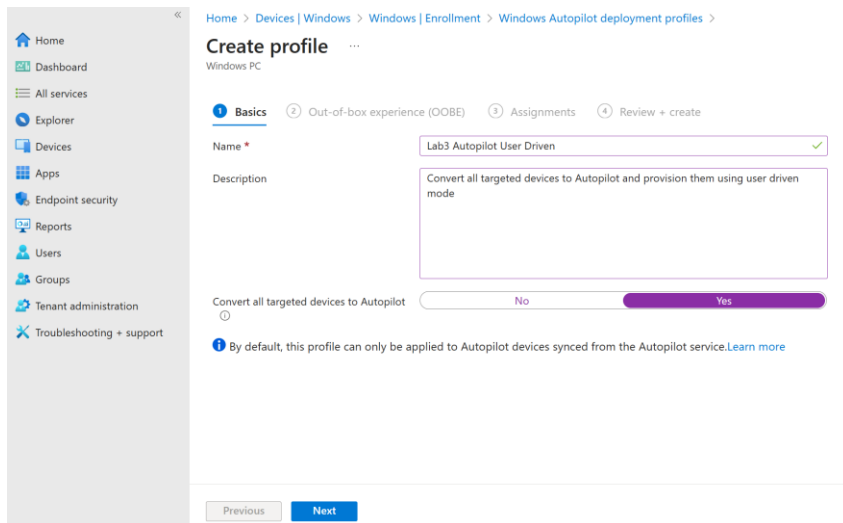
Lab 3 – Summary

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



The screenshot shows the 'Create profile' wizard in the Microsoft Intune console. The breadcrumb trail is: Home > Devices | Windows > Windows | Enrollment > Windows Autopilot deployment profiles >. The title is 'Create profile' with a dropdown arrow, and the subtitle is 'Windows PC'. The wizard has four steps: 1. Basics (selected), 2. Out-of-box experience (OOBE), 3. Assignments, and 4. Review + create. In the 'Basics' step, the 'Name' field is 'Lab3 Autopilot User Driven' with a green checkmark. The 'Description' field contains the text 'Convert all targeted devices to Autopilot and provision them using user driven mode'. Below this is a toggle switch for 'Convert all targeted devices to Autopilot', which is currently set to 'Yes'. A note at the bottom states: 'By default, this profile can only be applied to Autopilot devices synced from the Autopilot service. [Learn more](#)'. At the bottom of the form are 'Previous' and 'Next' buttons.

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)

The screenshot shows the 'Create profile' page for a Windows PC. The breadcrumb trail is: Home > Devices | Windows > Windows | Enrollment > Windows Autopilot deployment profiles >. The page title is 'Create profile' with a three-dot menu. Below the title is 'Windows PC'. The navigation tabs are: Basics (checked), Out-of-box experience (OOBE) (active), Assignments, and Review + create. The main heading is 'Configure the out-of-box experience for your Autopilot devices'. The configuration options are: Deployment mode (User-Driven), Join to Microsoft Entra ID as (Microsoft Entra joined), Microsoft Software License Terms (Show/Hide toggle), Privacy settings (Show/Hide toggle), Hide change account options (Show/Hide toggle), User account type (Administrator/Standard toggle), Allow pre-provisioned deployment (No/Yes toggle), Language (Region) (Operating system default), Automatically configure keyboard (No/Yes toggle), and Apply device name template (No/Yes toggle). At the bottom are 'Previous' and 'Next' buttons.

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

The screenshot shows the 'Create profile' page for a Windows PC. The breadcrumb trail is: Home > Devices | Windows > Windows | Enrollment > Windows Autopilot deployment profiles >. The page title is 'Create profile' with a three-dot menu. Below the title is 'Windows PC'. The navigation tabs are: Basics (checked), Out-of-box experience (OOBE) (checked), Assignments (active), and Review + create. The main heading is 'Included groups'. Below this are links for 'Add groups' and 'Add all devices'. A table shows the assignment: 'All devices' is listed under 'Groups', and there is a 'Remove' link next to it. At the bottom are 'Previous' and 'Next' buttons.

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

The screenshot shows the 'Create profile' page for a Windows PC. The left sidebar contains navigation links: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area shows the 'Create profile' page with a breadcrumb trail: Home > Devices | Windows > Windows | Enrollment > Windows Autopilot deployment profiles >. The page title is 'Create profile' with a three-dot menu icon. Below the title is 'Windows PC'. The 'Summary' section is followed by the 'Basics' section, which includes: Name (Lab3 Autopilot User Driven), Description (Convert all targeted devices to Autopilot and provision them using user driven mode), Convert all targeted devices to Autopilot (Yes), and Device type (Windows PC). The 'Out-of-box experience (OOBE)' section includes: Deployment mode (User-Driven), Join to Microsoft Entra ID as (Microsoft Entra joined), Skip AD connectivity check (No), Language (Region) (Operating system default), Automatically configure keyboard (Yes), Microsoft Software License Terms (Hide), Privacy settings (Hide), Hide change account options (Hide), User account type (Standard), and Allow pre-provisioned deployment (No). At the bottom are 'Previous' and 'Create' buttons.

Basics	
Name	Lab3 Autopilot User Driven
Description	Convert all targeted devices to Autopilot and provision them using user driven mode
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC
Out-of-box experience (OOBE)	
Deployment mode	User-Driven
Join to Microsoft Entra ID as	Microsoft Entra joined
Skip AD connectivity check	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No

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

The screenshot shows the Windows Out-of-Box Experience (OOBE) sign-in screen. The title is 'Let's set things up for your work or school'. Below the title is the text 'You'll use this info to sign in to your devices.' The Microsoft logo is displayed, followed by the 'Sign in' section. The email address 'Tim@portfolio006.onmicrosoft.com' is entered in the sign-in field. Below the sign-in field is a 'Sign-in options' link. At the bottom, there is a note: 'Choosing **Next** means that you agree to the Microsoft Services Agreement and privacy and cookies statement.' A 'Next' button is located at the bottom right.

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

Home > Devices | Overview >

Windows | Windows devices

Search

Refresh Export Columns Bulk device actions 1 devices

Windows devices

Monitor

Device onboarding

Windows 365

Enrollment

Manage devices

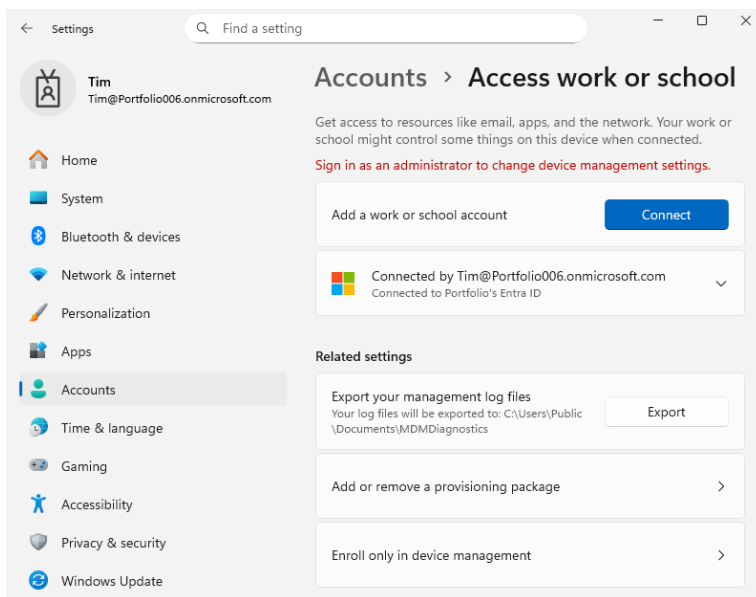
Configuration

Search

OS: Windows, Windows Mobile, Windows Holographic Add filters

Device name	Managed by	Ownership	Compliance	OS	OS version	Primary user UPN	Last check-in
TIMSCOMPUTE	Intune	Personal	Compliant	Windows	10.0.26100.6584	Tim@Portfolio0...	09/20/2025, 09:08 AM

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-4ddb-a240-24be39de2b10
AuthCodeUrl : https://login.microsoftonline.com/47db5d37-013b-4ddb-a240-24be39de2b10/oauth2/aut
horize
Access token URL : https://login.microsoftonline.com/47db5d37-013b-4ddb-a240-24be39de2b10/oauth2/tok
en
MdmUrl :
MdmUserUPN :
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-4ddb-a240-24be3
9de2b10/
WebAuthNSrvId : urn:ms-drs:enterpriseregistration.windows.net
DeviceManagementSrvVer : 1.0
DeviceManagementSrvUrl : https://enterpriseregistration.windows.net/manage/47db5d37-013b-4ddb-a240-24be39d
e2b10/
DeviceManagementSrvId : urn:ms-drs:enterpriseregistration.windows.net
KerbSpn : adrs/enterpriseregistration.windows.net
KerbUrl : https://login.microsoftonline.com/47db5d37-013b-4ddb-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.