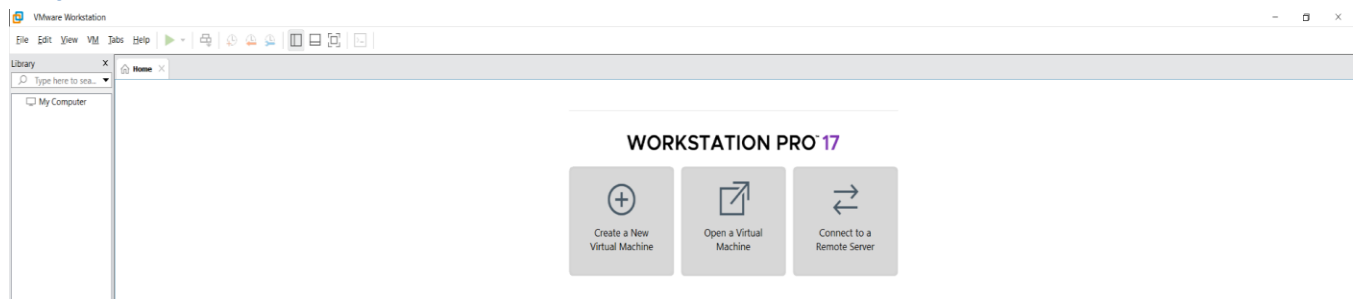


Lab 2 – Intune Enrollment (with Evidence on VMware)

Lab 2 – Summary

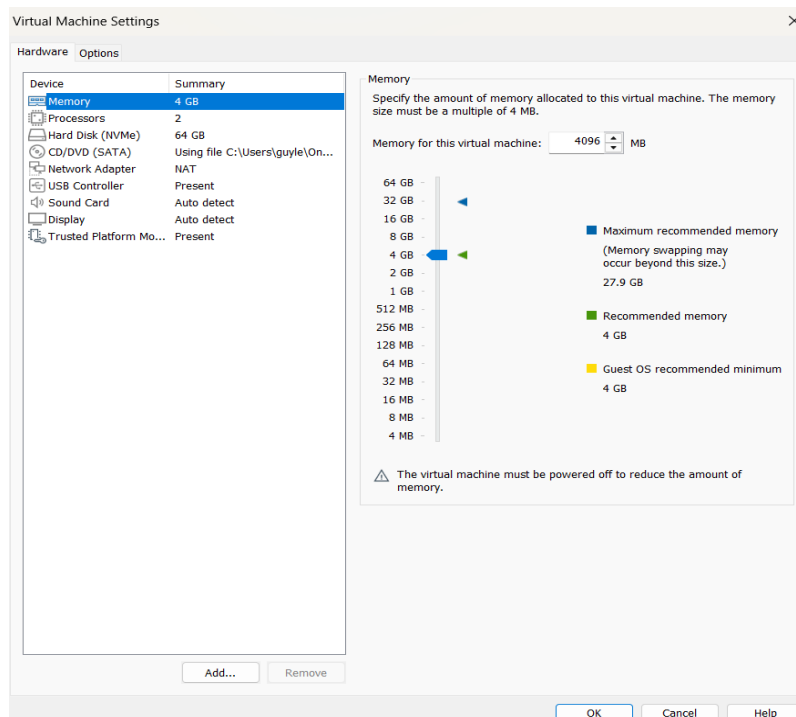
in this lab, I deployed a Windows 11 virtual machine with VMware Workstation, enrolled the device into Microsoft Intune via Entra ID, applied a password policy, and enforced least privilege by using a separate local admin account. Evidence is provided below.

Step 1 – Install VMware Workstation



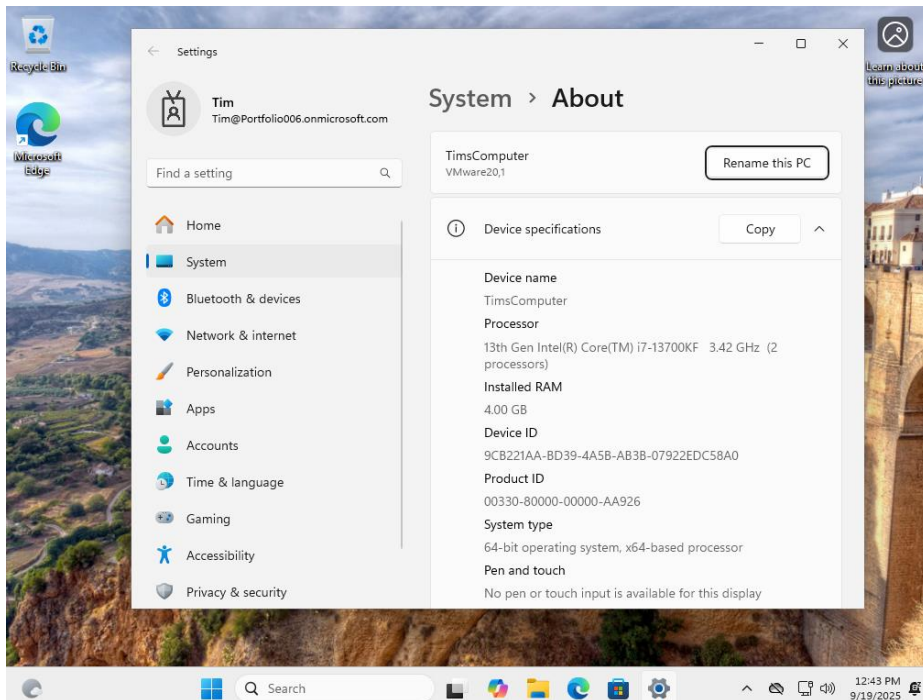
Notes: Installed VMware Workstation Pro 17 to host the Windows 11 virtual machine.

Step 2 – (Configure VM Settings)



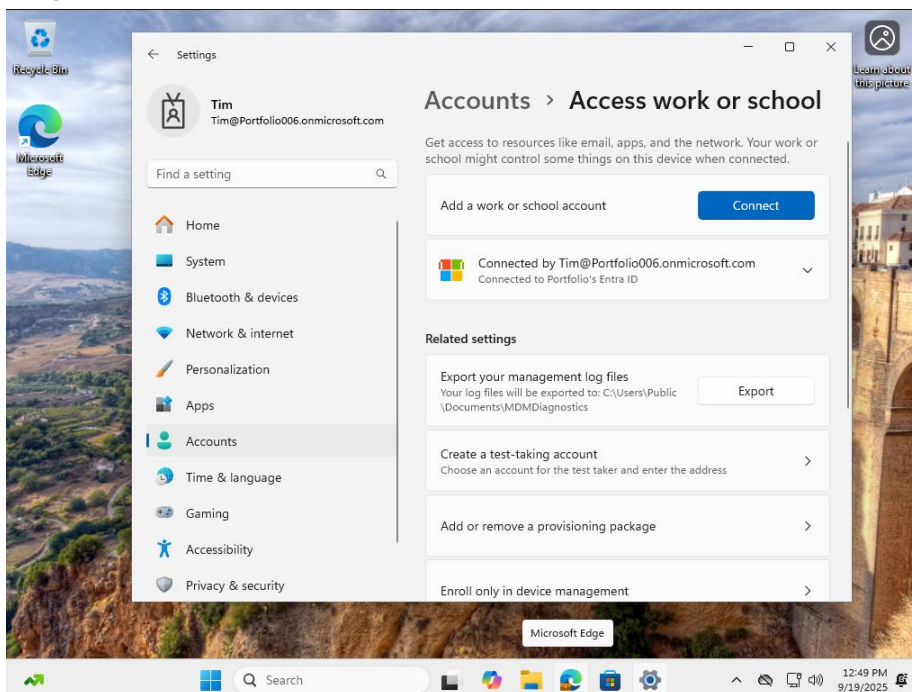
Notes: Configured VM hardware (RAM, CPU, disk) to meet Windows 11 requirements.

Step 3 – (Install Windows 11)



Notes: Installed Windows 11 Pro from the official ISO and verified OS details after setup, when launching on VM ware I selected my ISO file and the environment started to load.

Step 4 – (Connect Device to Entra ID / Intune)



Notes: Connected Tim's account under Settings → Accounts → Access work or school → Connect

Step 5 – (Device Registration & Sync)

Active users

Add a user Multi-factor authentication Refresh Delete user Reset password <input type="text" value="Search active users list"/>			
Filter set: Commonly used ⌵ Licenses Sign-in status Domain Location			
<input type="checkbox"/>	Display name ↑	Username	Licenses
<input type="checkbox"/>	Guy Cheneval	GuyCheneval@Portfolio006.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	LocalAdmin	LocalAdmin@Portfolio006.onmicrosoft.com	Microsoft 365 Business Premium
<input checked="" type="checkbox"/>	Tim	Tim@Portfolio006.onmicrosoft.com	Microsoft 365 Business Premium

Notes: Confirmed enrolment on Admin on Microsoft portal.

Home > Devices | Overview > Windows | Windows devices >

TIMSCOMPUTER

Search × ⏪ [Retire](#) [Wipe](#) [Delete](#) [Remote lock](#) [Sync](#) [Reset passcode](#) [Restart](#) [Fresh Start](#) [Autopilot Reset](#) [Quick scan](#) [Full scan](#) ⋮

Overview

- Manage
 - Properties
- Monitor
 - Resource explorer
 - Hardware
 - Discovered apps
 - Device compliance
 - Device configuration
 - App configuration
 - Recovery keys
 - User experience
 - Group membership
 - Managed Apps
 - Filter evaluation
 - Enrollment
 - Remediations (preview)

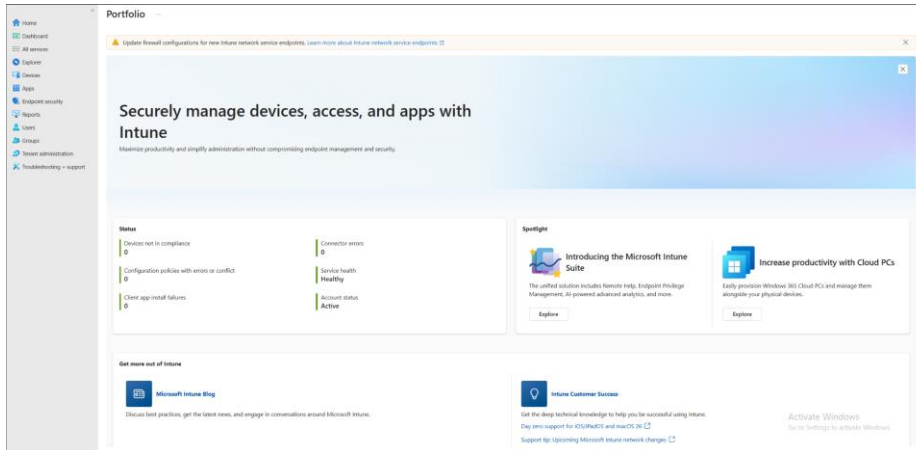
Essentials

Device name	: TIMSCOMPUTER	Primary user	: Tim
Management name	: Tim_Windows_9/19/2025_3:05 AM	Enrolled by	: Tim
Ownership	: Personal	Compliance	: Compliant
Serial number	: VMware-564d49d9a9b2d7e7-b2a073a1aa8669bc	Operating system	: Windows
Phone number	: ---	Device model	: VMware20,1
Device manufacturer	: VMware, Inc.	Last check-in time	: 9/19/2025, 3:31:22 PM
		Remote assistance	: Not configured

Action	Status	Date/Time	Error
No data			

Notes: Registered the device with Intune and performed a manual Sync. Confirmed the device appears and is compliant in Endpoint Manager.

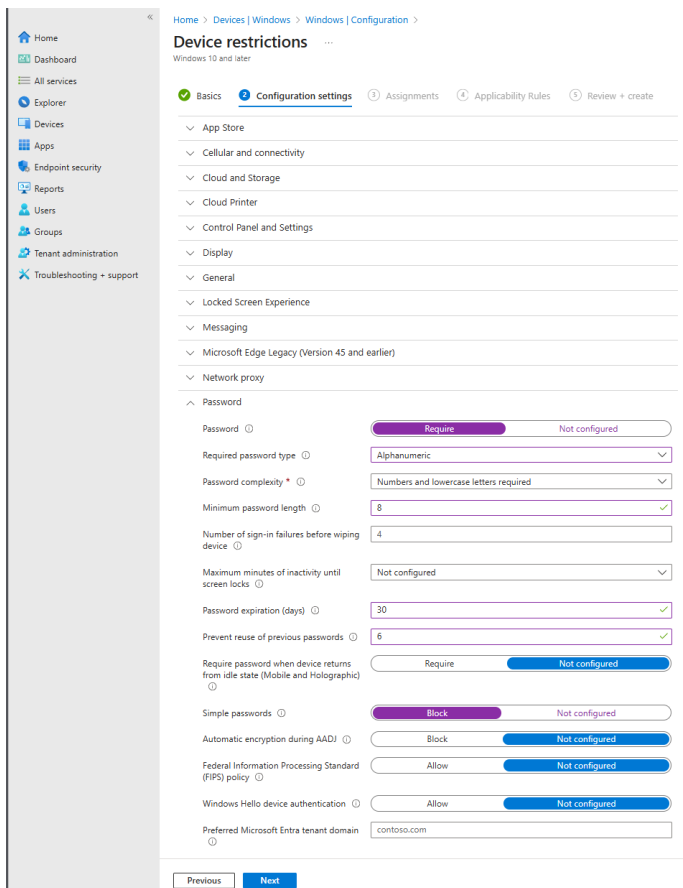
Step 6 – (Endpoint Manager Dashboard)



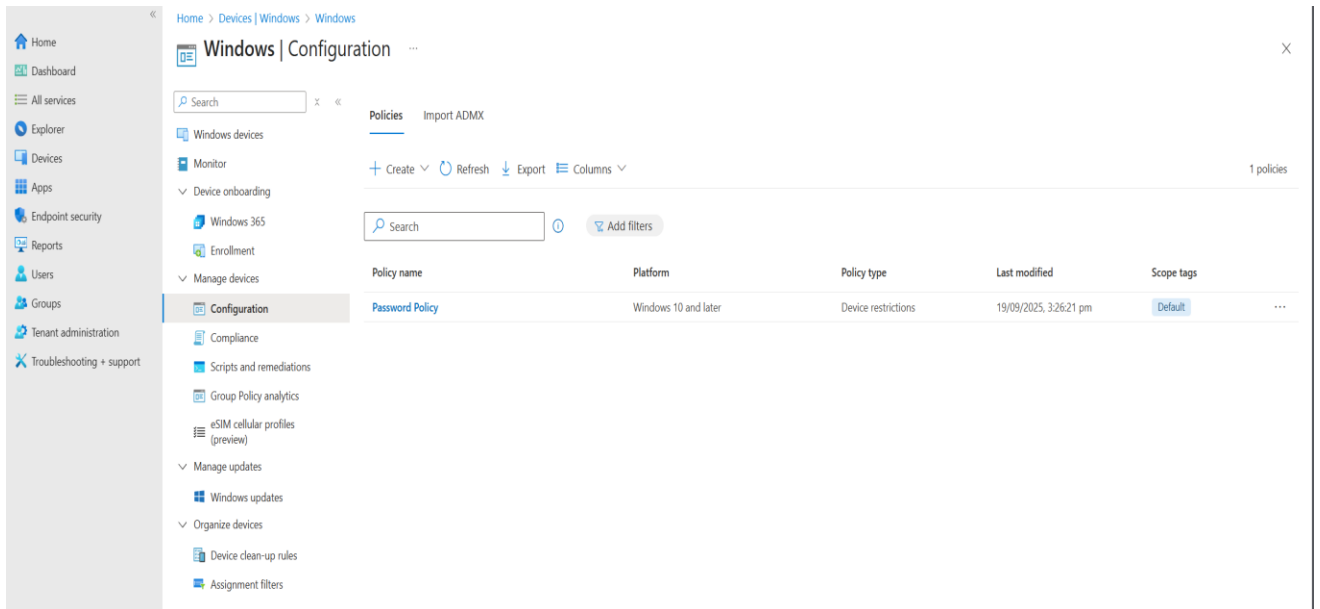
Notes: Verified

tenant health and device reporting from the Endpoint Manager dashboard.

Step 7 – Create Password Policy

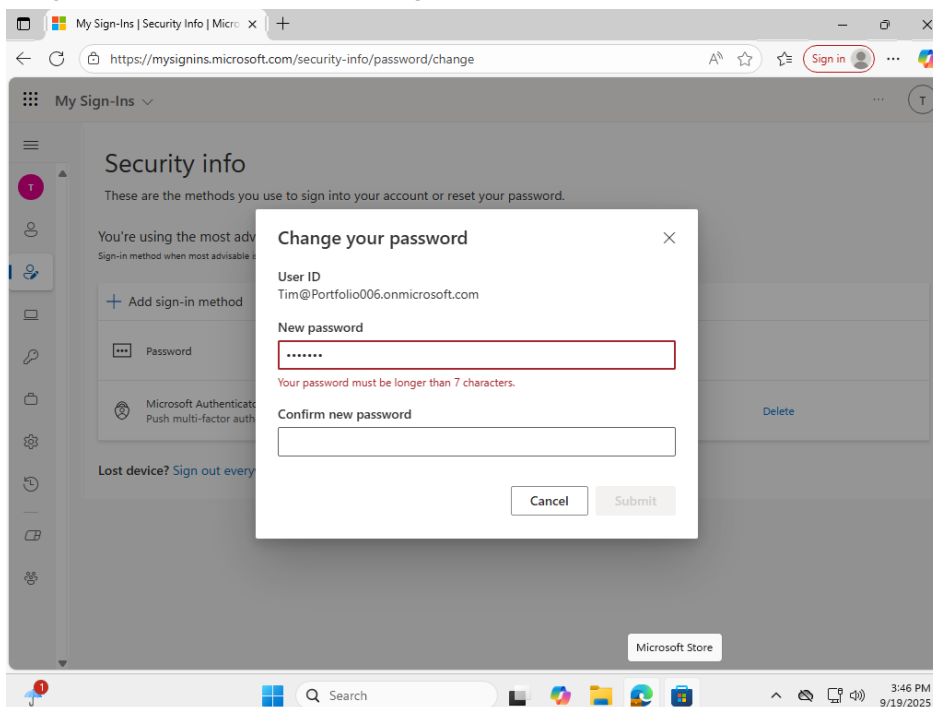


Notes: Navigated to the *Devices* section in Endpoint Manager and into the policy creation area for Windows. Here, I configured the password policy. I also noted that this section allows creation of many other policies, such as device restrictions, compliance settings, and security baselines.



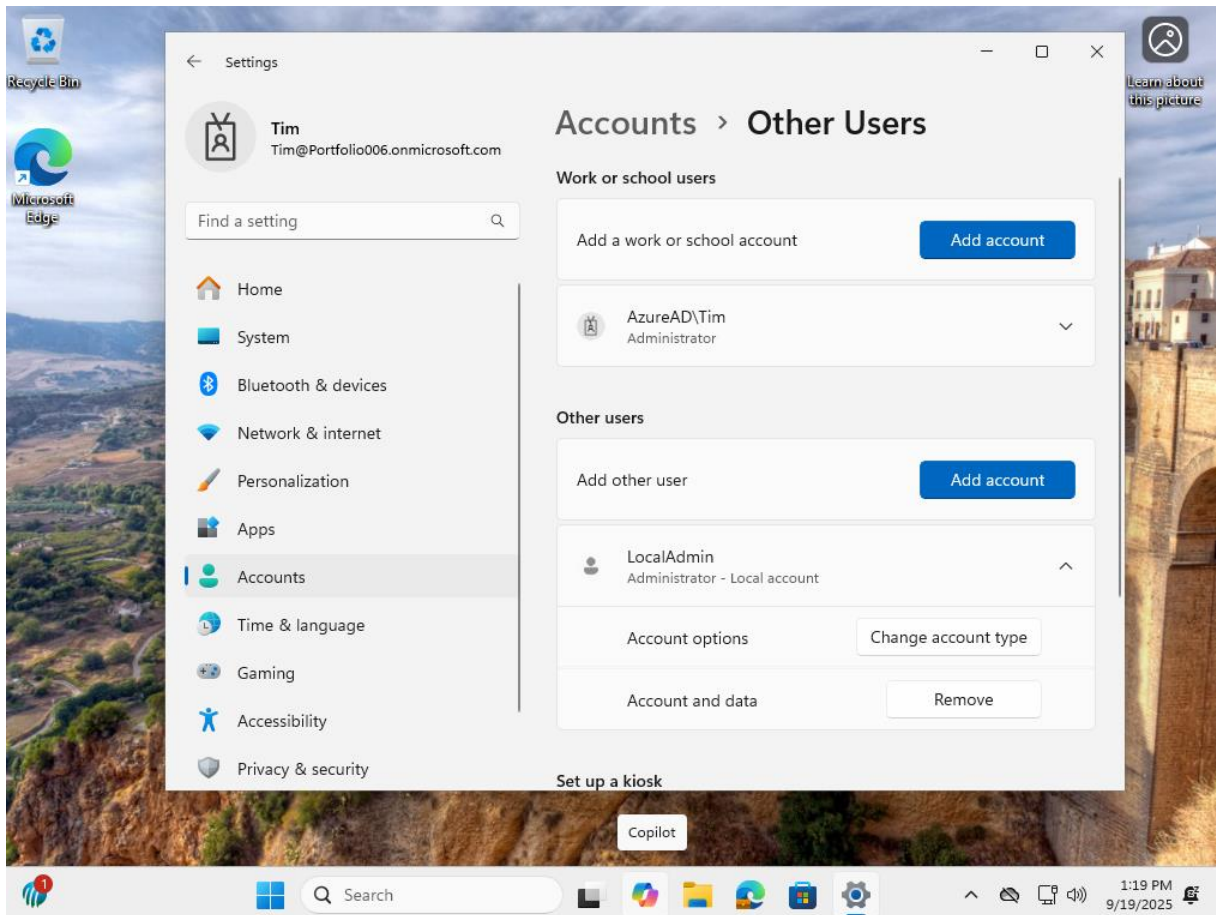
Notes: Created a Windows configuration profile that enforces a minimum password length of 8 characters, including complexity requirements such as numbers and lowercase letters. In addition, I applied best practices by enabling password expiry and restricting password reuse, further strengthening account security.

Step 8 – Test Password Policy Enforcement

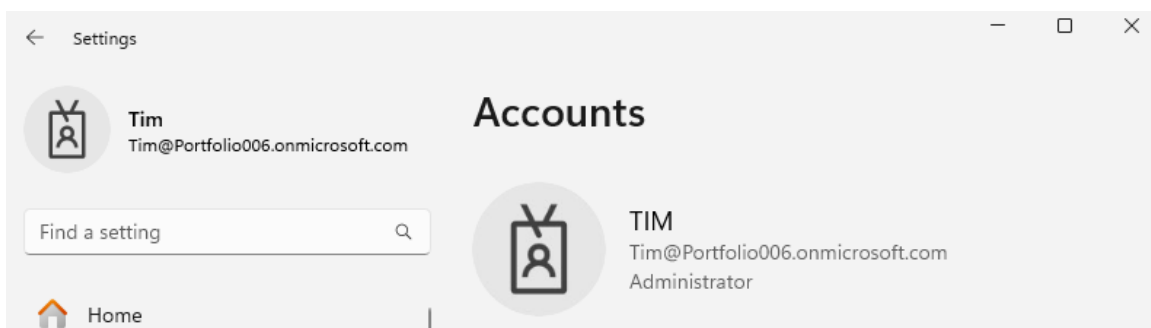


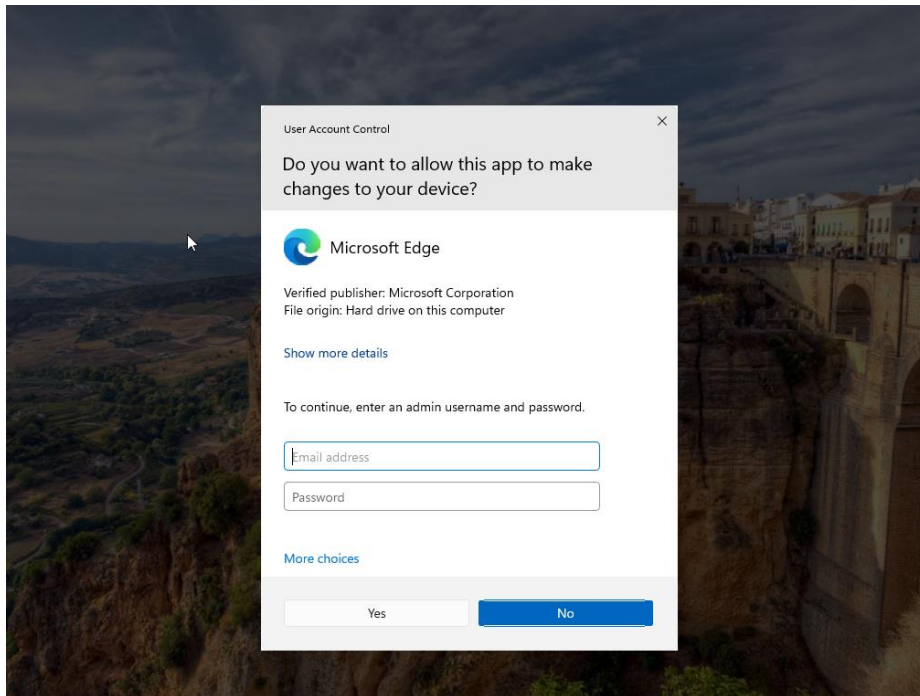
Notes: Attempted to set a weak password to test the new policy, which requires a minimum of 8 characters. The attempt was rejected, confirming that the policy was successfully enforced.

Step 9 – Admin Rights Check (Least Privilege)



Notes: An issue I ran into was Tim has Administrator right although his role-based access control said otherwise, to test this out I wanted to see if Tim could download a zip file and it turns out he could.





Notes: To fix the issue, I created a separate Local Admin account and downgraded Tim's account to a standard user. When testing again, any attempt to open programs requiring elevation prompted Tim to enter admin credentials, confirming least privilege was enforced.

Summary for Lab - 2

In this lab, I set up a Windows 11 virtual machine in VMware, connected it to Microsoft Entra ID, and enrolled it into Intune. I created and applied a password policy through Endpoint Manager, which enforced strong password rules and blocked weak ones.

I also fixed an issue where the test user had admin rights by creating a separate local admin account and making the user a standard account. This confirmed that least privilege was enforced while the device stayed compliant in Intune.