BYOD Policy Overview and Policy Document

Overview

This project was conducted to design, implement, and validate a secure Bring Your Own Device (BYOD) program for TechSecure Innovations, a company that has recently adopted a BYOD initiative. The goal of the program is to enable employees to use personal laptops and mobile devices for work, while maintaining strict security and privacy standards for corporate data.

BYOD environments introduce several security risks:

Potential malware infections or outdated devices.

Data leakage through personal apps or unsecured storage.

Unauthorized access if a device is lost, stolen, or shared.

Lack of encryption or strong authentication.

The risk of rooted/jailbroken devices bypassing protections.

To address these risks, Microsoft Intune MDM was implemented as the management solution. Using Intune, robust Compliance Policies and App Protection Policies were deployed, along with a formal BYOD Policy that governs all employee participation.

This policy ensures that corporate data is protected while respecting employee privacy, enabling a balance between flexibility and security.

BYOD Policy

Acceptable Use Guidelines

Employees may use personal laptops and mobile devices to access approved corporate applications and resources. Appropriate use includes accessing:

Email (Outlook)

Corporate file storage (OneDrive for Business)

Collaboration tools (Microsoft Teams)

Approved internal systems

Prohibited use includes:

Installing or using unauthorized software to access corporate data.

Circumventing or disabling security controls.

Using corporate resources for illegal or personal commercial activities.

Sharing corporate access credentials with unauthorized persons.

Security Configurations Required

Participation in the BYOD program requires the following mandatory configurations:

Full-disk encryption enabled at all times (BitLocker on Windows, File-Based Encryption on Android).

A strong password/PIN must be configured:

Minimum 6 characters.

Complex format recommended.

Device lockout after failed attempts.

Device must be enrolled in Microsoft Intune via the Company Portal app.

Separation of corporate and personal data is enforced through Intune App Protection Policies.

Device Compliance Requirements

To remain compliant, personal devices must meet the following criteria:

Maintain full-disk encryption.

Enforce strong password/PIN policy.

Devices must not be rooted or jailbroken.

The operating system must be up to date with security patches.

Non-compliant devices will be blocked from corporate access until remediated.

Data Protection Policies

Corporate data must only be accessed through approved applications and protected as follows:

Corporate data must not be saved to personal storage.

Copy/paste between corporate and personal apps is restricted.

Data cannot be shared to personal cloud storage or unauthorized services.

Upon employee separation or program exit, corporate data will be remotely wiped from enrolled devices.

Monitoring Guidelines

Monitoring of personal devices is strictly limited to corporate security needs:

Only corporate app usage and device compliance status are monitored.

The company does not access personal data, photos, texts, apps, or usage.

No location tracking is performed for personal devices.

Employees retain full ownership and control of their personal devices.

Employee Acknowledgment Process

BYOD participation is voluntary. To participate, employees must:

Review this BYOD Policy.

Sign an Employee BYOD Acknowledgment Form.

Consent to device enrollment and management through Microsoft Intune.

Maintain ongoing compliance with this policy.

Failure to comply may result in:

Loss of corporate access.

Removal from the BYOD program.

Possible disciplinary action for deliberate violations.

My Process for Enrolling Emily Johnson's BYOD Device (VM) into Intune

For this project, I tested BYOD (Bring Your Own Device) enrollment into Microsoft Intune using a Windows 10 virtual machine (VM) in Hyper-V.

My test user is Emily Johnson:

Email: Emily.Johnson@akfash161.onmicrosoft.com

Step 1: Preparing Emily's Account

First, I prepared the user account for enrollment:

I verified that Emily Johnson exists in Microsoft Entra ID (Azure AD).

I assigned her a Microsoft 365 Business Premium license, which includes Intune.

In the Intune admin center, under Mobility (MDM and MAM) → Microsoft Intune, I configured the following settings:

MDM user scope: All

Windows Information Protection (WIP) user scope: None

Note: During my testing, I discovered that setting WIP user scope to None was important. When WIP was enabled, the enrollment process would not complete successfully.

Step 2: Setting Up the VM

For this test, I created a Windows 10 VM in Hyper-V.

I used the Default Switch for networking.

Although some documentation recommends using an External Switch to provide full network access, in this case, I used Default Switch and proceeded with the test.

Step 3: Installing Company Portal

Inside the VM, I completed the following steps:

I opened Microsoft Edge.

I navigated to https://aka.ms/companyportal.

I downloaded and installed the Company Portal app.

I launched the Company Portal app after installation.

Step 4: Enrolling Emily's Device

In the Company Portal app:

On the sign-in screen, I entered: Emily.Johnson@akfash161.onmicrosoft.com

I entered Emily's password and completed multi-factor authentication (MFA) as required.

The app prompted me to "Add work account to this device."

I clicked "Add work account" and followed the on-screen instructions to allow device management and complete the enrollment process.

Step 5: Enrollment Outcome

After completing the enrollment process:

The VM was registered in Azure AD as Azure AD Registered, which is correct for a BYOD scenario (not Azure AD Joined).

The device was enrolled in Microsoft Intune.

The device appeared under Devices → All Devices in the Intune admin center.

Any assigned compliance policies were successfully applied to the device.

Step 6: Verification

To verify successful enrollment, I performed the following:

I logged into the Microsoft Intune admin center.

I navigated to Devices → All Devices.

I searched for Emily Johnson’s device.

I confirmed the following details:

Join type: Azure AD Registered

MDM: Microsoft Intune

Compliance: Compliant (based on assigned policy).

Final Notes (My Observations)

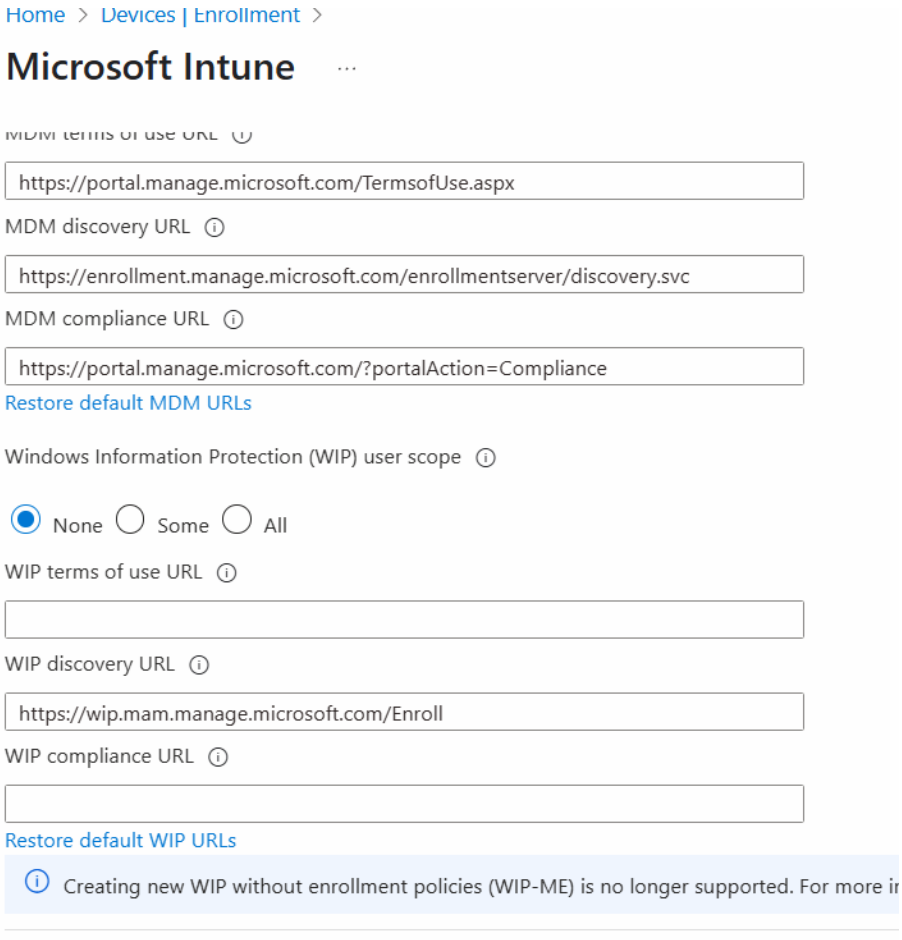
Even though I used Default Switch in Hyper-V, the enrollment process completed successfully after I set the WIP user scope to None.

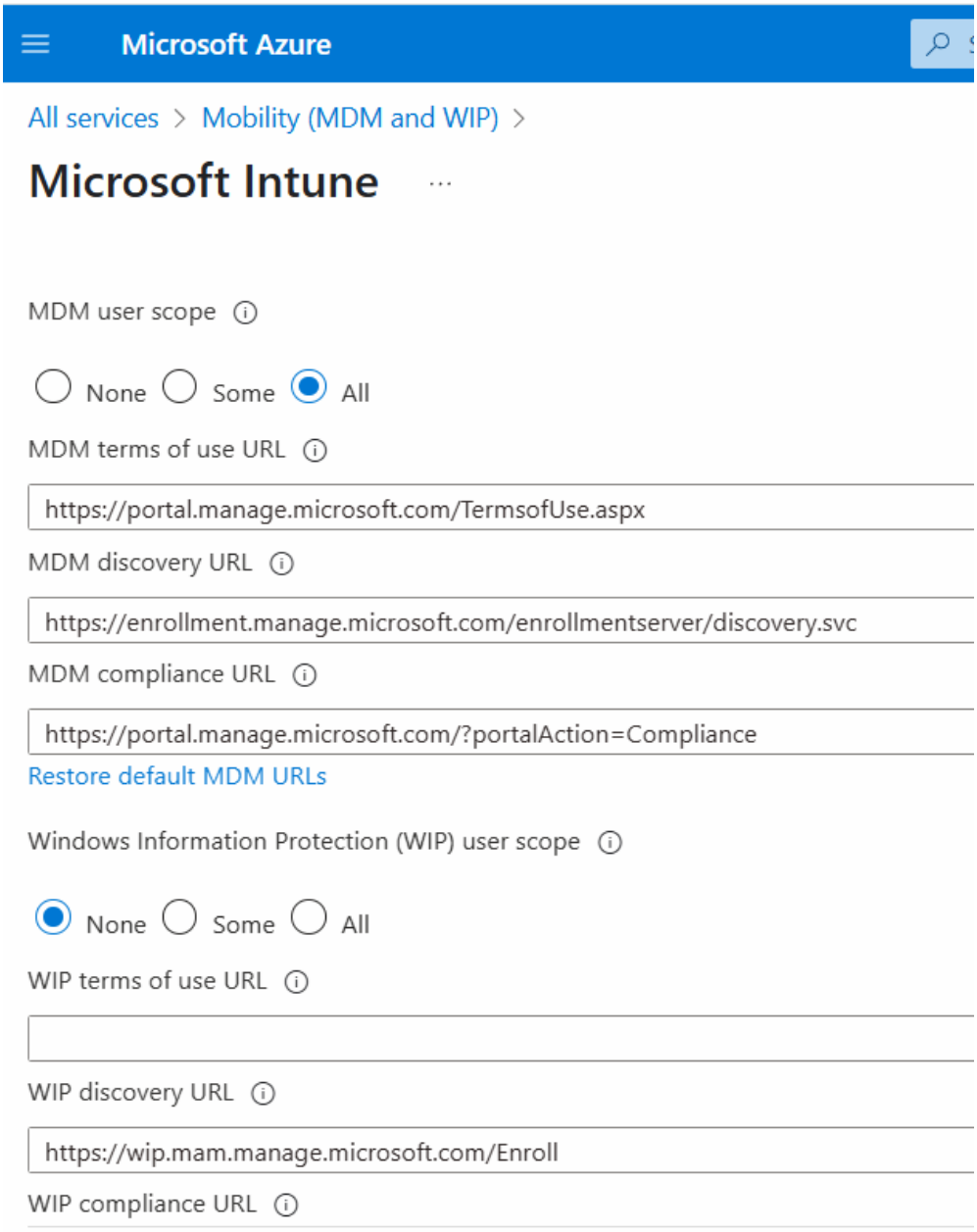
In my earlier tests, when WIP was enabled, the Company Portal would get stuck at "checking your account."

Once I changed the WIP user scope to None, I restarted the process and enrollment worked properly, even with Default Switch.

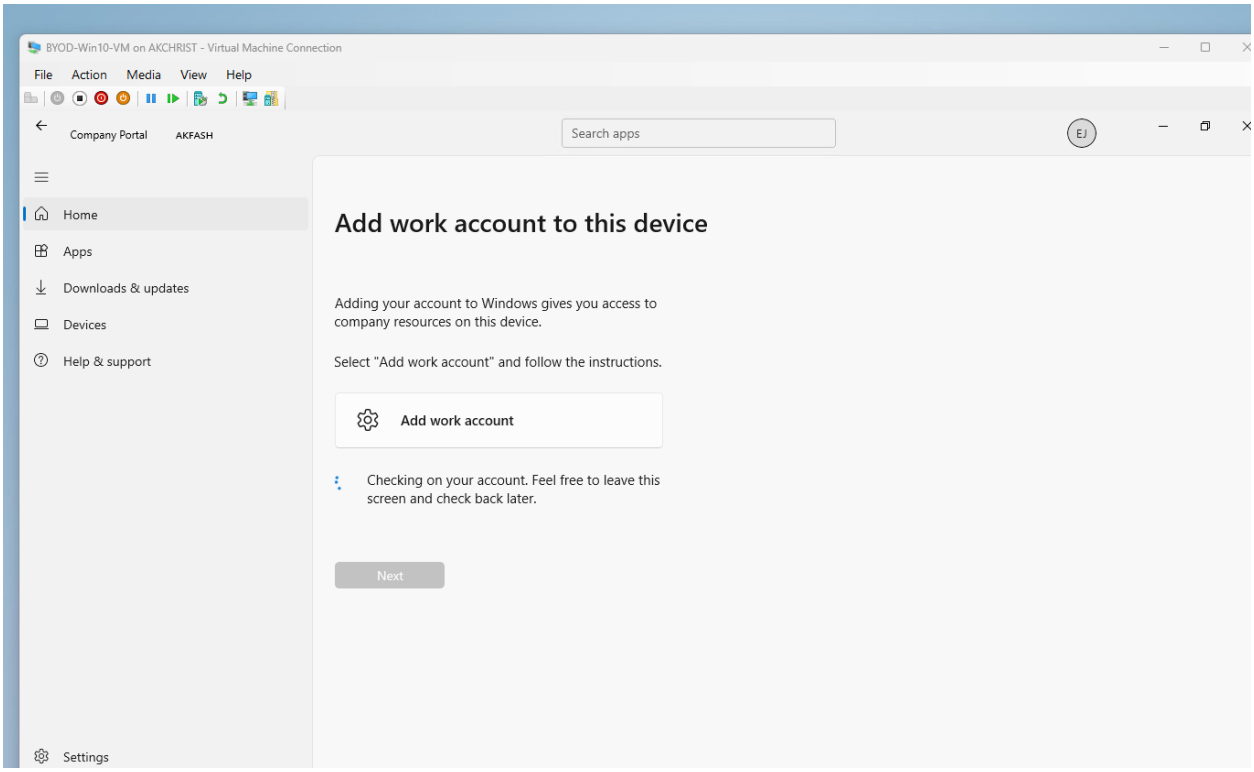
This test confirmed that for BYOD Windows devices (including virtual machines), having WIP enabled can interfere with enrollment. For BYOD scenarios, it is best to leave WIP disabled unless there is a specific requirement to use it.

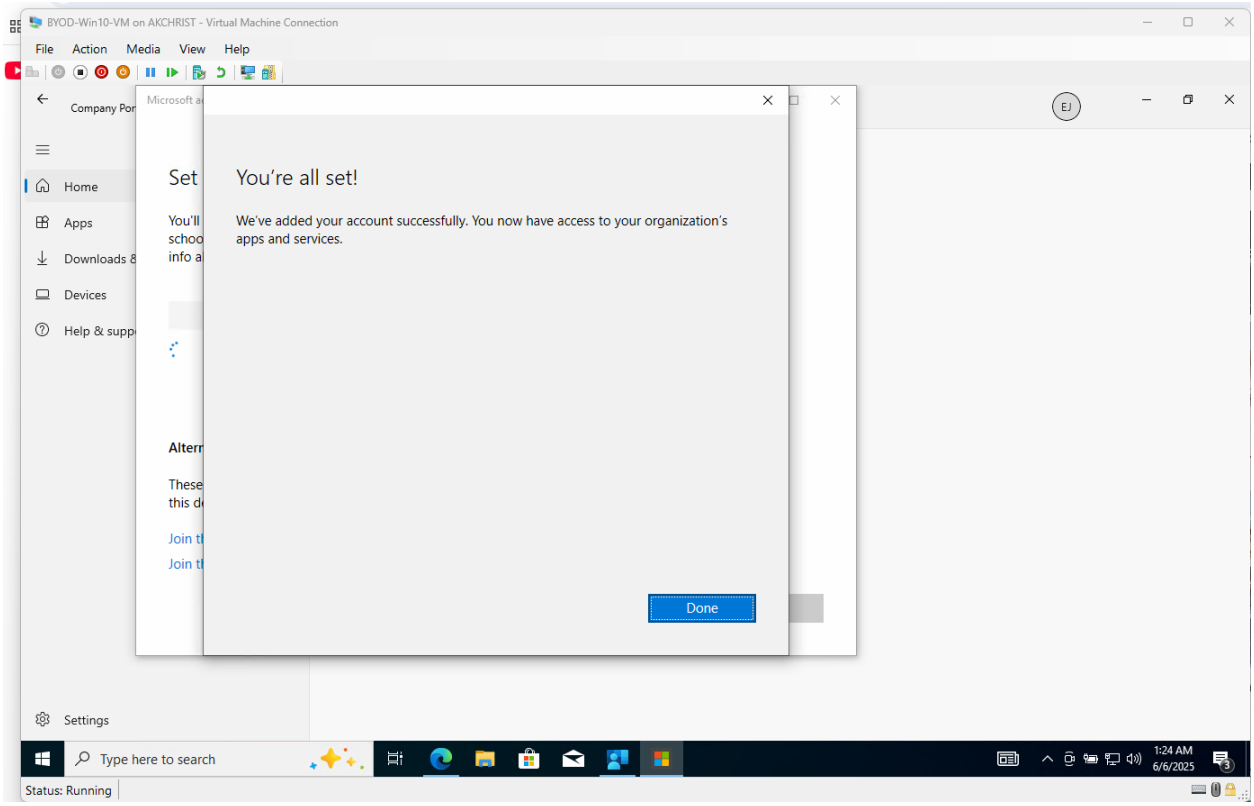
Screenshot of setting Windows Information Protection (WIP) user scope on Intune and Azure to none in order to prevent the system from trying to apply WIP policies which can break BYOD flow especially on VMs:

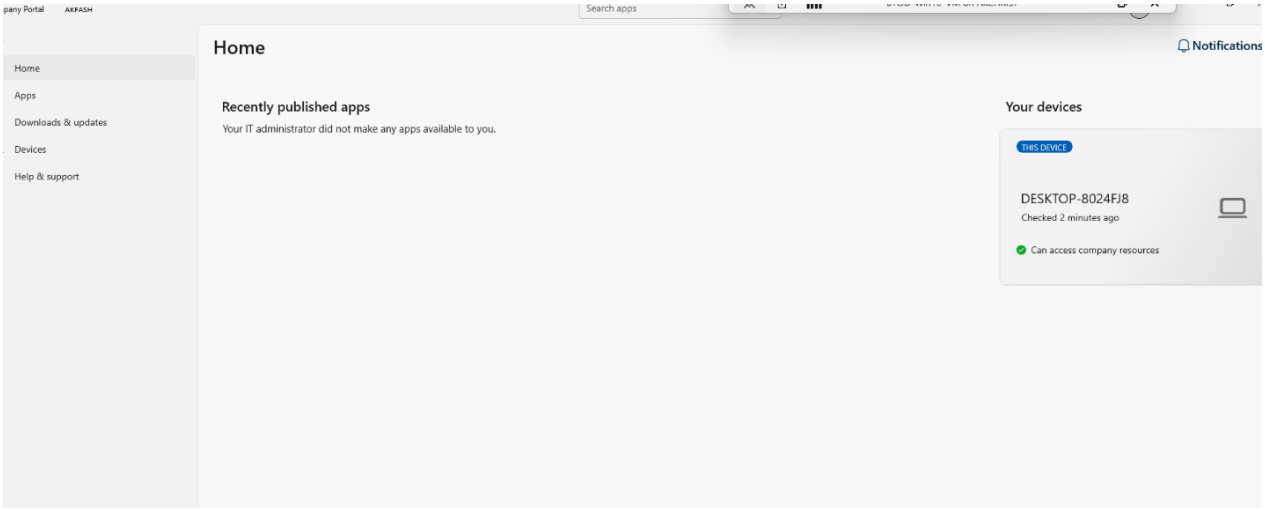


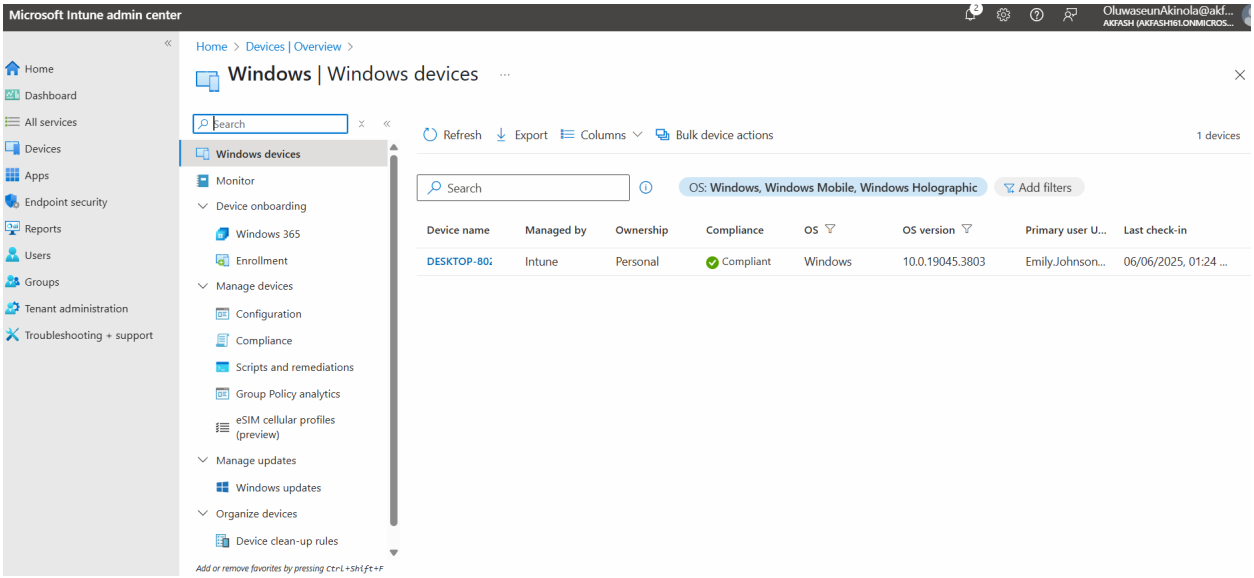


Screenshot showing device is successfully added:

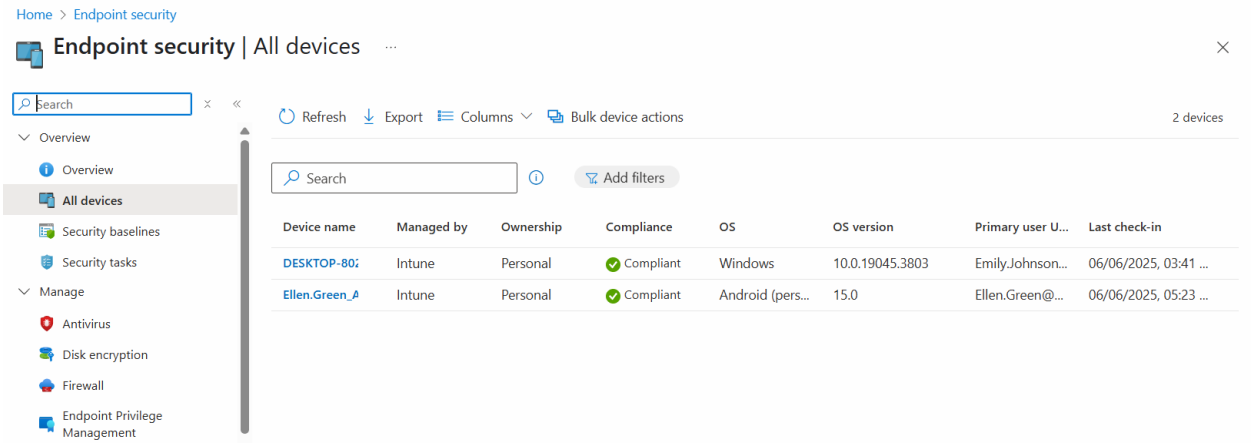

BYOD-Win10-VM on AKCHRIST - Virtual Machine Connection
File Action Media View Help
Company Portal AKFASH
Search apps
EJ
Home
Apps
Downloads & updates
Devices
Help & support
Settings
Add work account to this device
Adding your account to Windows gives you access to company resources on this device.
Select "Add work account" and follow the instructions.
Add work account
Checking on your account. Feel free to leave this screen and check back later.
Next

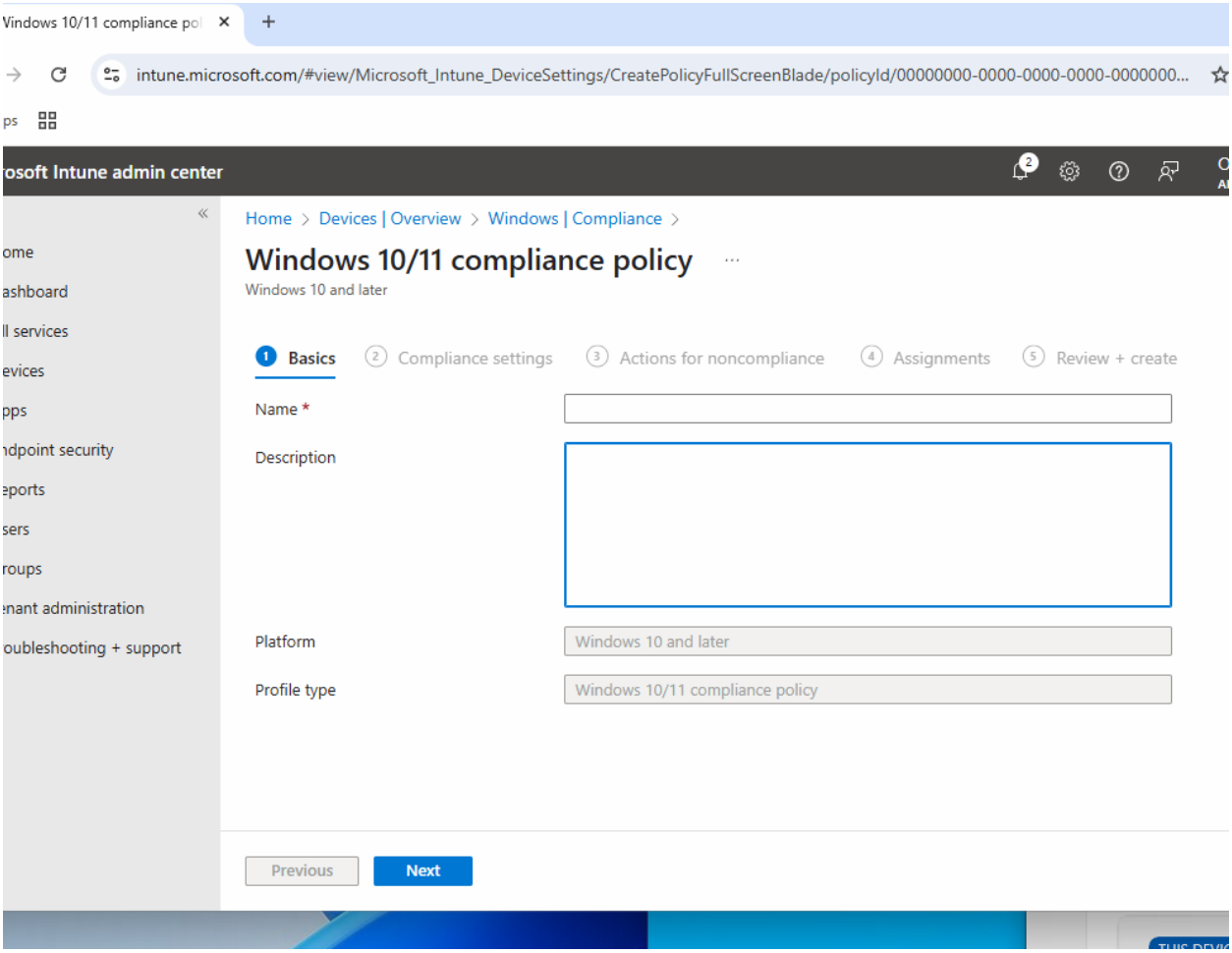

BYOD-Win10-VM on AKCHRIST - Virtual Machine Connection
File Action Media View Help
You're all set!
We've added your account successfully. You now have access to your organization's apps and services.
Done
Settings
Type here to search
1:24 AM
6/6/2025
Status: Running

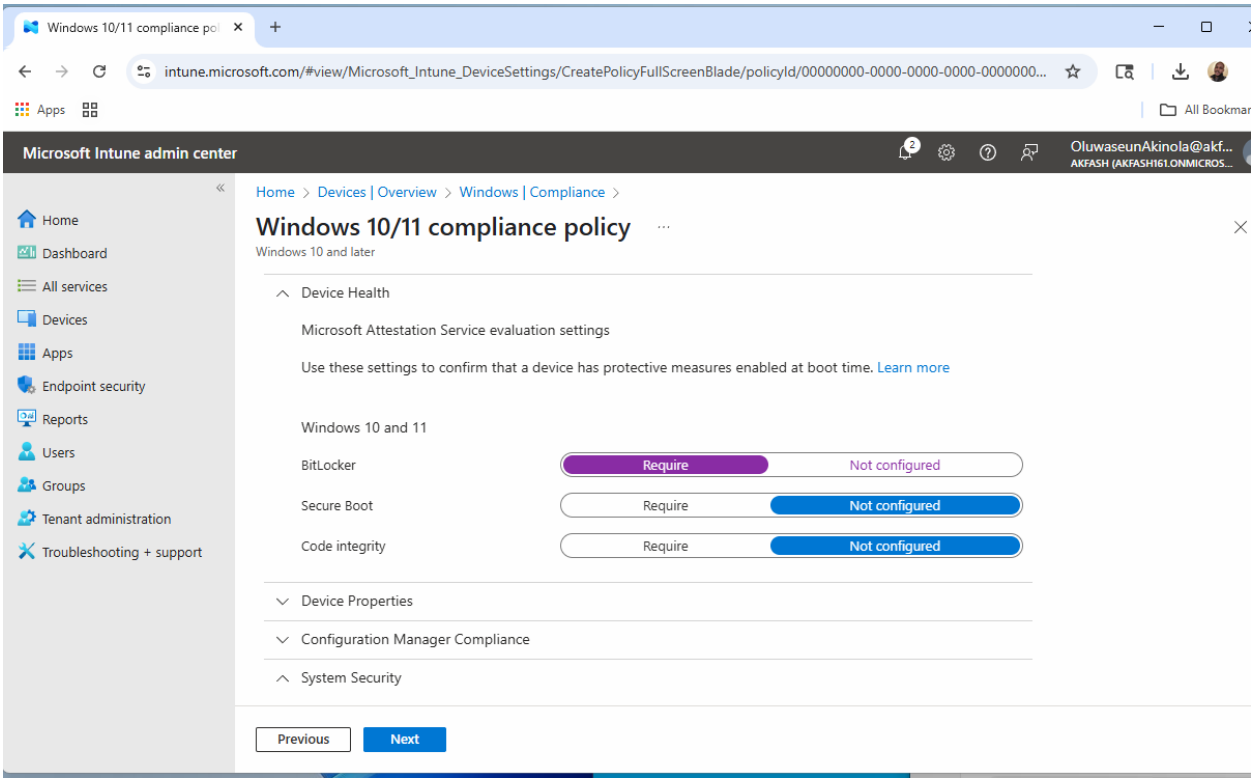


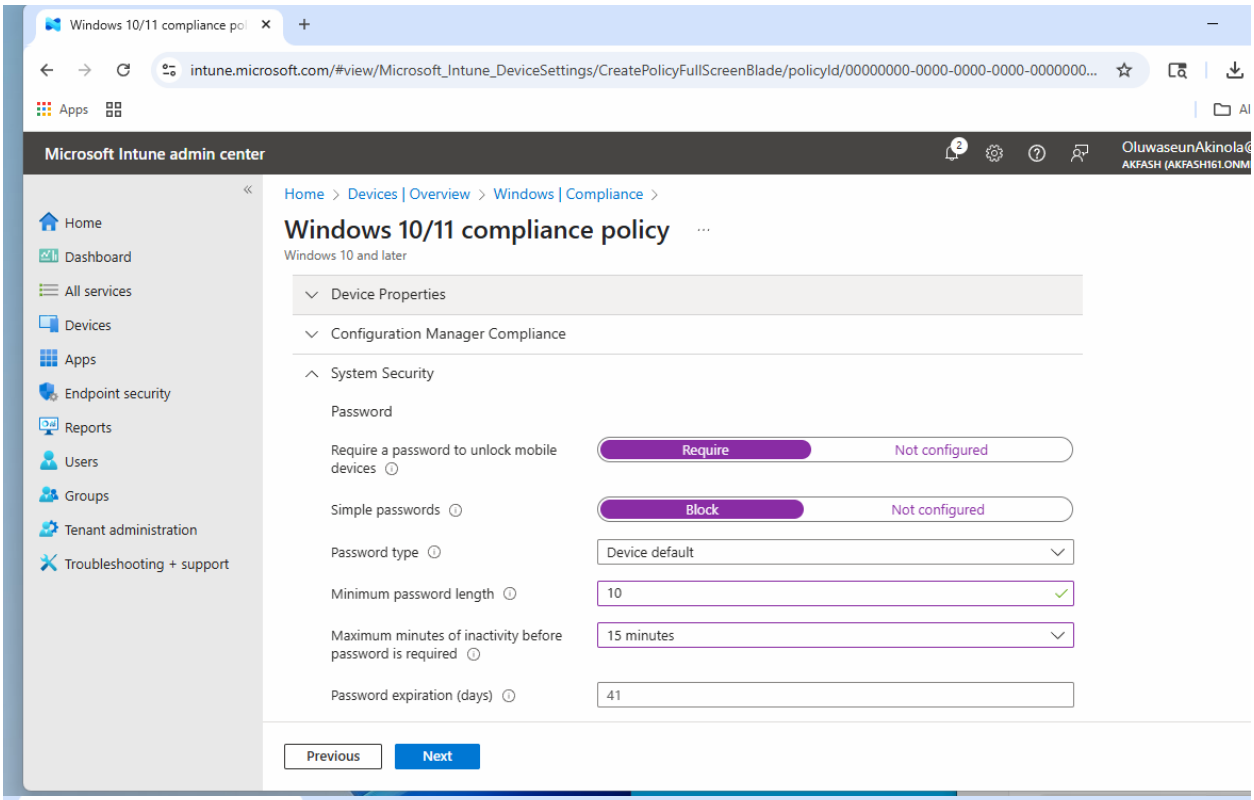


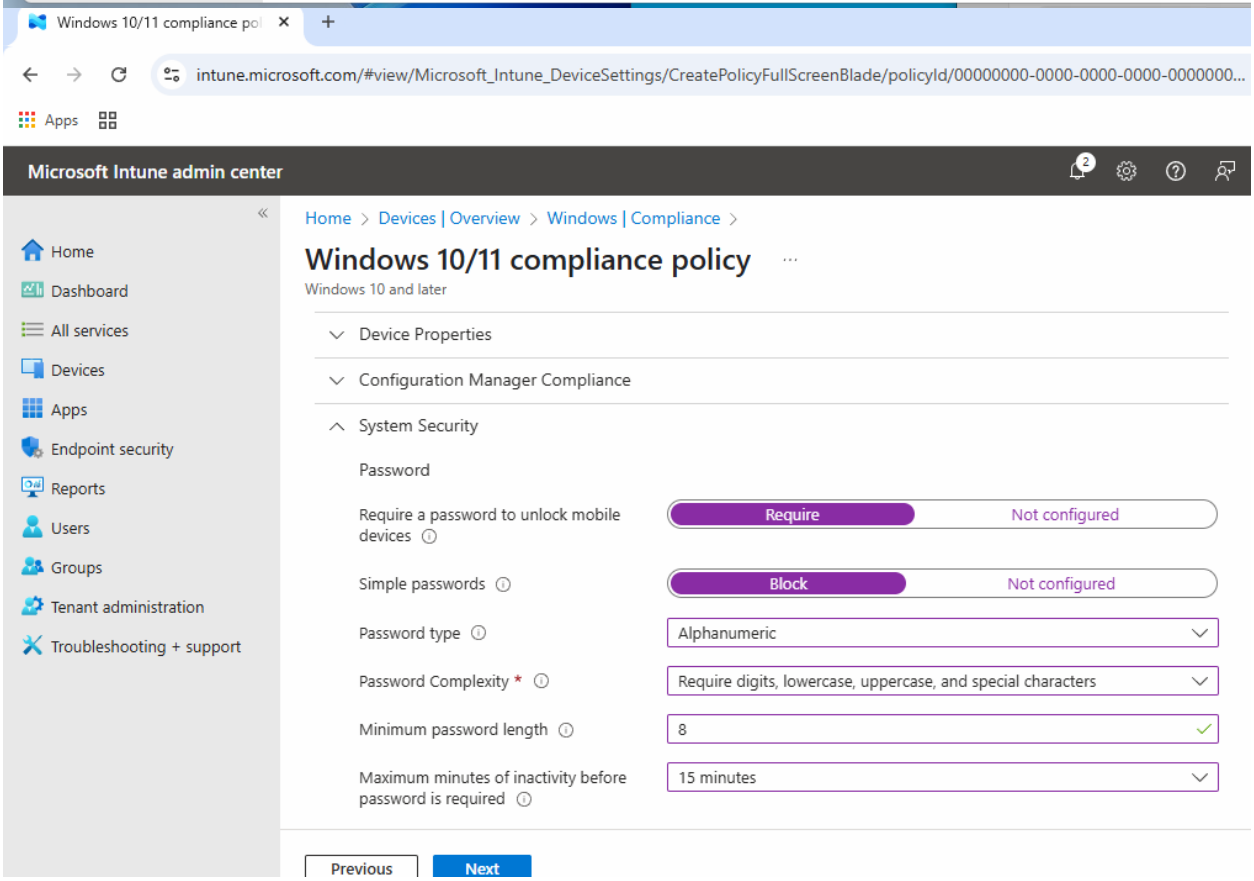
Screenshot showing both devices are compliant:


Home > Endpoint security
Endpoint security | All devices
Search
Overview
Overview
All devices
Security baselines
Security tasks
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Refresh
Export
Columns
Bulk device actions
2 devices
Search
Add filters
Device name
Managed by
Ownership
Compliance
OS
OS version
Primary user U...
Last check-in
DESKTOP-80:
Intune
Personal
Compliant
Windows
10.0.19045.3803
Emily.Johnson...
06/06/2025, 03:41 ...
Ellen.Green_A
Intune
Personal
Compliant
Android (pers...
15.0
Ellen.Green@...
06/06/2025, 05:23 ...


Windows 10/11 compliance pol
intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/CreatePolicyFullScreenBlade/policyId/00000000-0000-0000-0000-0000000...
osoft Intune admin center
Home > Devices | Overview > Windows | Compliance >
Windows 10/11 compliance policy
Windows 10 and later
1 Basics
2 Compliance settings
3 Actions for noncompliance
4 Assignments
5 Review + create
Name *
Description
Platform
Windows 10 and later
Profile type
Windows 10/11 compliance policy
Previous
Next


Windows 10/11 compliance pol
intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/CreatePolicyFullScreenBlade/policyId/00000000-0000-0000-0000-0000000...
Apps
All Bookmar
Microsoft Intune admin center
OluwaseunAkinola@akf...
AKFASH (AKFASH161.ONMICROS...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Overview > Windows | Compliance >
Windows 10/11 compliance policy
Windows 10 and later
Device Health
Microsoft Attestation Service evaluation settings
Use these settings to confirm that a device has protective measures enabled at boot time. Learn more
Windows 10 and 11
BitLocker
Require
Not configured
Secure Boot
Require
Not configured
Code integrity
Require
Not configured
Device Properties
Configuration Manager Compliance
System Security
Previous
Next


Windows 10/11 compliance pol
intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/CreatePolicyFullScreenBlade/policyId/00000000-0000-0000-0000-0000000...
Apps
Microsoft Intune admin center
OluwaseunAkinola@
AKFASH (AKFASH161.ONM
Home > Devices | Overview > Windows | Compliance >
Windows 10/11 compliance policy
Windows 10 and later
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Device Properties
Configuration Manager Compliance
System Security
Password
Require a password to unlock mobile devices
Require
Not configured
Simple passwords
Block
Not configured
Password type
Device default
Minimum password length
10
Maximum minutes of inactivity before password is required
15 minutes
Password expiration (days)
41
Previous
Next


Windows 10/11 compliance pol
intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/CreatePolicyFullScreenBlade/policyId/00000000-0000-0000-0000-0000000...
Apps
Microsoft Intune admin center
Home > Devices | Overview > Windows | Compliance >
Windows 10/11 compliance policy
Windows 10 and later
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Device Properties
Configuration Manager Compliance
System Security
Password
Require a password to unlock mobile devices
Require
Not configured
Simple passwords
Block
Not configured
Password type
Alphanumeric
Password Complexity *
Require digits, lowercase, uppercase, and special characters
Minimum password length
8
Maximum minutes of inactivity before password is required
15 minutes
Previous
Next

Android device enrolled:

To enroll the Android device into Microsoft Intune, I first prepared my device — in this case, a personal Android smartphone running version 15.0. I made sure that my user account had an Intune license assigned through the Microsoft 365 Admin Center.

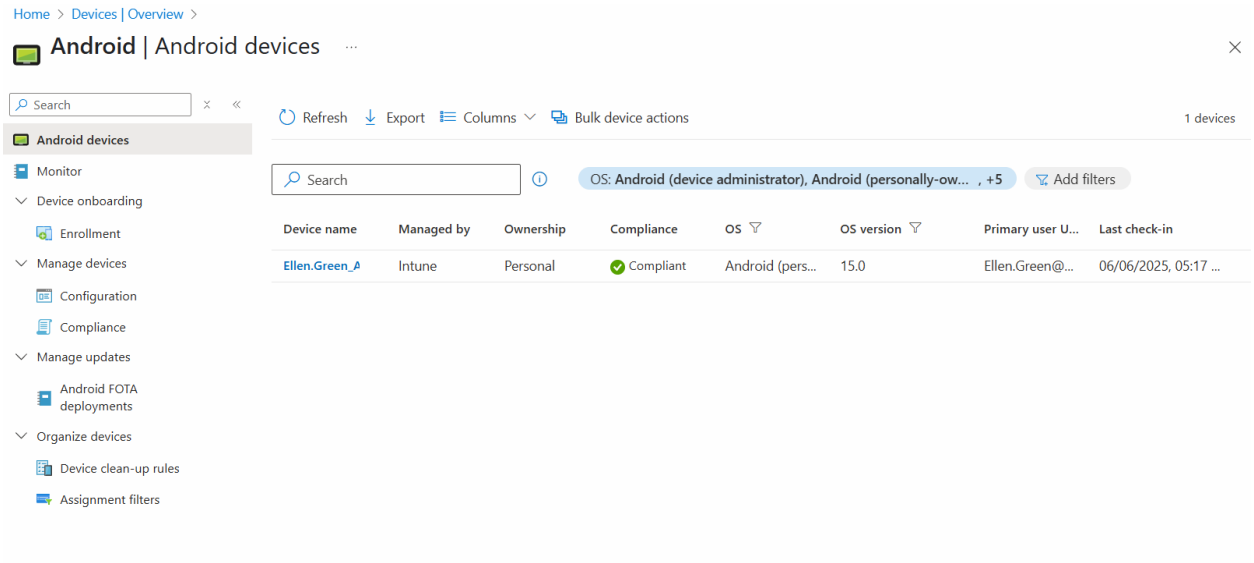
Next, I opened the Google Play Store on my phone and downloaded the Intune Company Portal app. Once the app finished installing, I launched it and signed in with my work account credentials (in this example, Ellen.Green@...). After completing multi-factor authentication, I proceeded to the device registration process.

The Company Portal guided me through several screens that explained what the organization can and cannot see on my device. I carefully reviewed the privacy information and accepted the terms. Then, I began setting up the Work Profile — since this is a BYOD scenario and I wanted to ensure personal data would remain separate from corporate data.

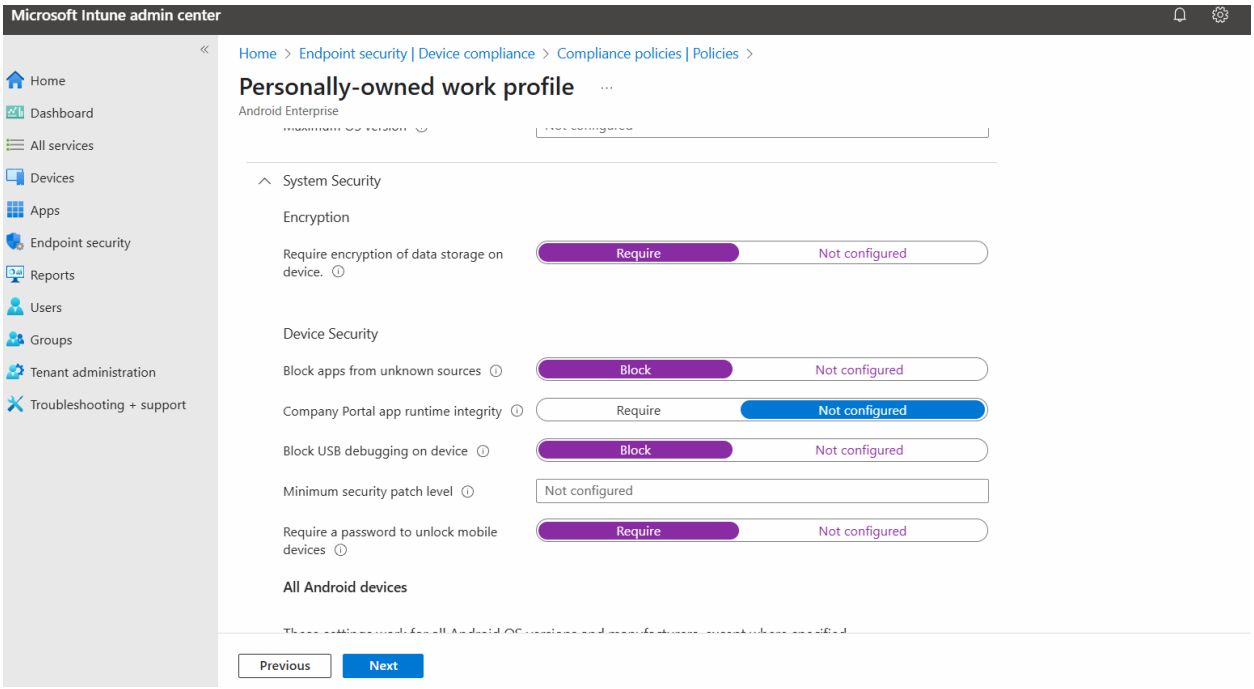
Once I started the setup, Android created a Work Profile on my phone. I waited while the necessary components were installed. After that, the app requested a few permissions, such as device admin access, and I approved them. It also required me to enforce certain security settings, like enabling encryption and setting a strong PIN/password. Once all the steps were complete, the Company Portal app displayed a confirmation screen letting me know that my device was successfully enrolled.

To ensure that everything synced properly, I opened the app's menu and selected the Sync option. After waiting a few moments, I logged into the Intune Admin Center through the web portal at https://intune.microsoft.com. I navigated to Devices → Android → Android Devices and confirmed that my device was now listed in the portal. The device showed as managed by Intune, personally-owned with a Work Profile, and marked as Compliant.

Screenshot showing android device added.



Screenshot showing compliance policy on android device:



Lessons Learned

Throughout this project, several common challenges arose. Setting up the Microsoft Intune trial and assigning licenses correctly took extra time to troubleshoot. Enrolling devices, especially the Android smartphone, required careful attention to platform selection and understanding where devices would appear in the Intune portal. Applying compliance and app protection policies also

involved multiple sync attempts before changes were fully reflected on the devices. Testing policy enforcement, such as verifying encryption or blocking rooted devices, required patience and careful validation.

For future BYOD implementations, clear documentation, consistent device management practices, and additional security measures like Conditional Access would help improve both efficiency and protection.