PHASE 3: Microsoft Intune Integration & Windows Autopilot Provisioning

This phase documents the configuration and deployment of Microsoft Intune as the Mobile Device Management (MDM) authority for DipeshCorp (*Alias of **nxhz***), the creation of endpoint security policies, manual Windows 11 device enrollment, and automated provisioning using Windows Autopilot. These steps emulate a modern device lifecycle workflow in a cloud-native enterprise environment.

I. Establishing Microsoft Intune as the MDM Authority

Enable Microsoft Intune as the MDM authority to manage Windows endpoint devices through Microsoft Endpoint Manager.

Actions Completed:

1. Logged in to Microsoft Endpoint Manager Admin Center:
    - URL: https://endpoint.microsoft.com
    - Admin account used: admin@dipeshcorp.onmicrosoft.com
2. Navigated to: Tenant Administration → Tenant Status → Tenant Details
3. Verified that the MDM Authority was set to: Microsoft Intune
4. **If not then,**

    Step 1: Verified License Assignment for Admin Account

    - Logged into Microsoft 365 Admin Center: https://admin.microsoft.com
    - Navigated to: Users → Active Users → admin@dipeshcorp.onmicrosoft.com
    - Under Licenses and Apps:
        - Confirmed that Microsoft 365 E5 Developer license was assigned

- Located “Microsoft Intune” within the apps list
- Initially unchecked — manually enabled it and saved changes

⚠️ Note: If “Microsoft Intune” is not checked, Intune will not initialize. Activation may take 5–10 minutes after enabling the checkbox.

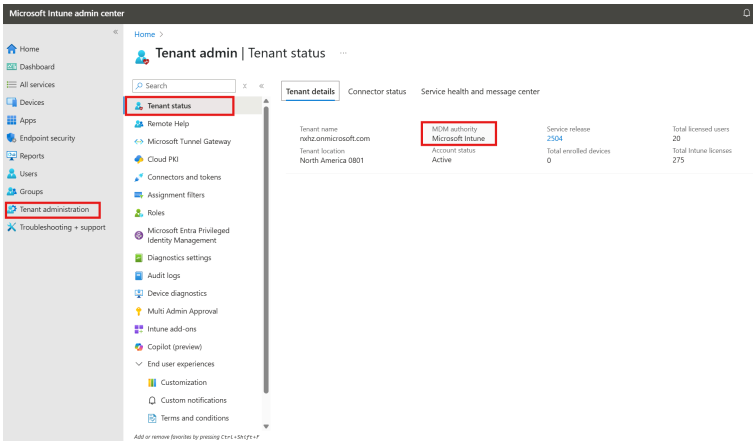
Step 3: Confirmed MDM Settings via Azure Portal

- Logged into Azure Portal: https://portal.azure.com
- Navigated to: Azure Active Directory → Mobility (MDM and MAM)
- Clicked “Microsoft Intune”
- Confirmed that it opened successfully
- Assigned scope: All users
- Clicked Save

This confirmed that Intune is now officially registered as the MDM provider, equivalent to setting MDM Authority manually.

Validation:

1. Refreshed the Tenant Administration page
2. Confirmed status: MDM Authority = Microsoft Intune



II. Creation of Intune Configuration Profile for Security Hardening

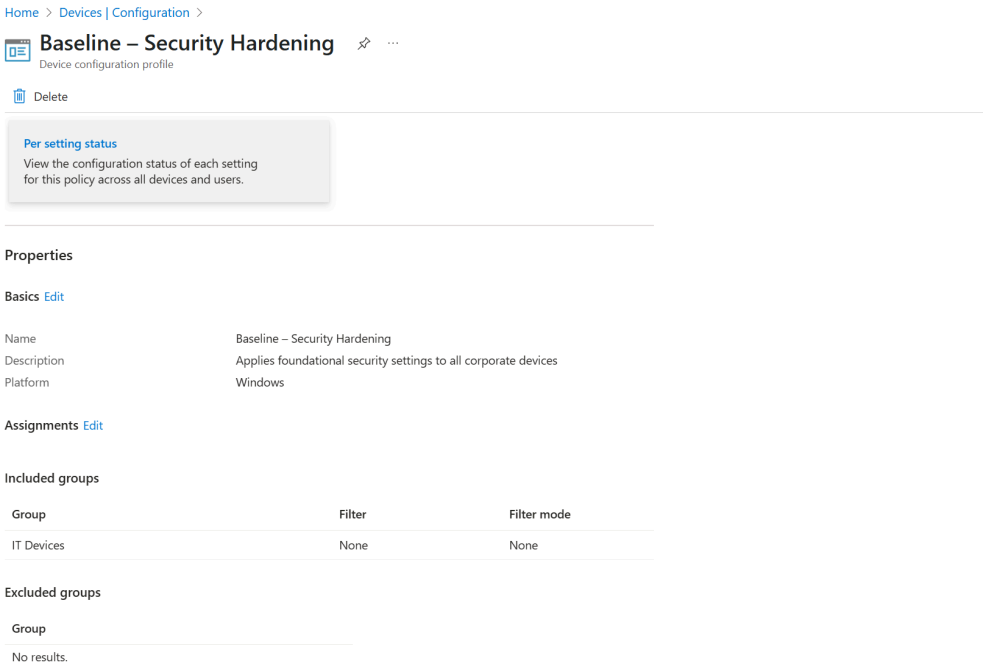
Enforce baseline security settings for all managed Windows 10/11 devices via policy-based management.

Actions Completed:

1. Navigated to:
    - Endpoint Manager > Devices > Under Manage Devices > Configuration
    - Clicked: + Create > New Policy
2. Profile Settings Configured:
    - Platform: Windows 10 and later
    - Profile Type: Settings Catalog > Clicked: Create
    - Name: Baseline – Security Hardening
    - Description: Applies foundational security settings to all corporate devices
3. Configuration Settings > + New Settings Added:
    - Device Lock > Device Password Enabled > In Alphanumeric Device Password Required: Min Device Password Complex Characters
    - Microsoft Defender Antivirus: Enable real-time protection
    - BitLocker: Require encryption on the system drive
4. Assignments:
    - Created Security Group: IT Devices
    - Microsoft 365 Admin Center Portal > Active Teams & Groups > Security Groups > Add a Security Group > Name: IT Devices
    - Assigned the profile to “IT Devices” group

Validation:

1. Opened the profile summary screen
2. Confirmed settings applied and scope assignment active



III. Manual Enrollment of Windows 11 Test Device

Enroll a Windows 11 device manually into Intune to validate MDM authority, policy assignment, and compliance reporting.

Actions Completed:

1. Provisioned a virtual machine named: Win11-VM01
   - Hypervisor: Hyper-V
   - Media: [Windows 11 ISO (Evaluation Edition)]
   - Encountered an error: “This system does not meet the minimum requirements for Windows 1”

   🛑 Root Cause: Hyper-V virtual machines require the Trusted Platform Module (TPM) to be enabled in order to meet Windows 11 hardware compatibility requirements.

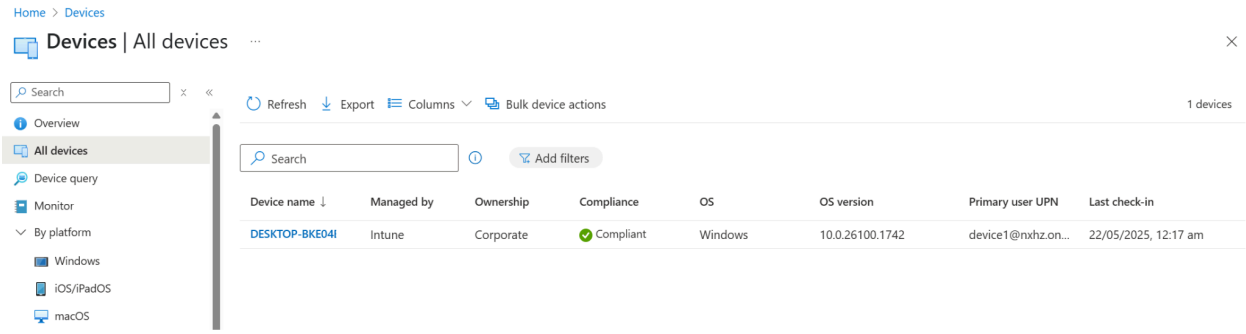
✔️ Resolution:

- Opened Hyper-V Manager
- Right-clicked Win11-VM01 > Settings
- Navigated to: Security > Enabled "Trusted Platform Module"
- Confirmed Secure Boot is enabled (also required for Windows 11)
- Restarted installation → Setup proceeded successfully
- Completed Windows 11 installation and initial configuration

2. Logged into Windows 11 with Web Credentials
3. Enrolled Device via Microsoft Work or School Account:
   - Start > Settings > Accounts > Access work or school > Connect
   - Entered credentials: device1@dipeshcorp.onmicrosoft.com
   - Completed MFA verification
   - Device registered successfully
4. Returned to: https://endpoint.microsoft.com
   - Navigated to: Devices > All Devices
   - Verified listing of Win11-VM01

Validation:

5. Checked compliance status based on previously assigned profile
6. Status: Compliant / Not Compliant based on profile effectiveness and BitLocker status



IV. Windows Autopilot Configuration for Zero-Touch Provisioning

Automate device provisioning by uploading hardware hash, assigning Autopilot deployment profiles, and simulating enterprise deployment.

Actions Completed:

Step 1: Configure Company Branding

1. In the Microsoft Entra admin center, navigate to Company branding
2. Customize default sign-in experience with your organization's logo, background images, and color schemes to enhance user experience during device setup

Step 2. Create an Autopilot Devices Group

1. In the Microsoft Entra admin center, go to Groups > All groups > New group
2. Set:
    - Group type: Security
    - Group name: e.g., "Windows Autopilot Devices"
    - Membership type: Dynamic Device
3. Add a dynamic membership rule:
    - DeviceOSType | Equals | Windows
    - And | DeviceOSVersion | Start With | 10.0.2 (For Windows 11)
4. Validate Rules (Preview)
    - Add devices which are connected and validate all devices to make sure this rule applies to them.

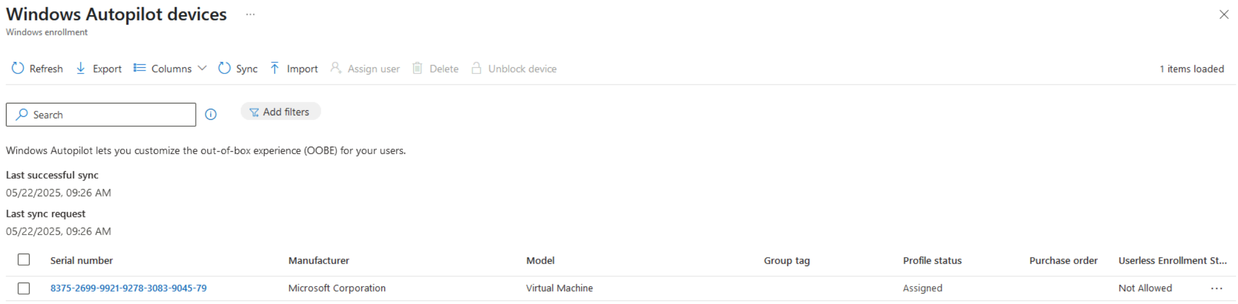
Step 3. Register Devices for Autopilot

1. Collect hardware IDs from devices using PowerShell:
    - Install-Script -Name Get-WindowsAutopilotInfo -Force

- Set-ExecutionPolicy RemoteSigned -Scope Process -Force
- Get-WindowsAutopilotInfo.ps1 -OutputFile AutopilotHWID.csv

```
Device Serial Number,Windows Product ID,Hardware Hash
8375-2699-9921-9278-3083-9045-79,,T0FOBAEAHAAAAAoANwb0ZQAACgDOBvRlv2TBL+QCCQkCABAACQABAAQACAABAAAABQAZAAYAAAAAAAAAAAAgAAAAAAAACAAEAAwMAEQBBdXRoZW50aWNBTUQABA
A0AEFNRCBSeXplbiA5IDU5MDBIUyB3aXRoIFJhZGVvbiBHcmFwaGljcyAgICAgICAgAAYAEACIAAAAAAAAAAoA/wEHAB4AfFZpcnR1YWwgRGlzayAgICB8TXNmdCAgICAIAB4AAAAAAAAAVXURCBAwAAABWAE
0AQgBVAFMAAAAJABAA///////////////GwAIAP////8JABAAAAAAAAAAEAAP/////GwAIAAAAAAAAKAAkAAwIBAAANAFYAVFBNLVZlcnNpb246Mi4wIC1MZXZlbDowLVJldmlzaW9uOjEuMTYtVmVuZG9ySU
Q6J01TRlQnLUZpcm13YXJlOjUzODI0NzQ0My4xMzk0NzIyABkABAHCO/crLEl2bvjMbOdj04zBYIDw16QRa6HswpgEwMBM+WdR8LTy1fNVKahZniWw7Ozz4BoP/
+A17y226tEJBRCRvDAgONkYeaVW73MuP19GhztlHKi72TbGd8yovMpffFRCZWgsOdHcNEHnUju8j3QKiszp/nOcmhFBC1sJouQ8Igw6FLYP1x8EDDOQrRLQ/7rm1LnG7hGi+xPb9JJfHDMo9zsvIpv3S1OIX
6IBPsOWY40K6OgEdpjjk2uCEyBmY4q+
9MHjY+ZdXnGDyn2HSegVnc+Kazep2zixLOAOHLvcNu6bmNWeBn7HmCS+QQ0Q3flpu/6L6EgTRpif21JjQ3ijCwAuAAAAAAABACAAAABirKjtrh7oO/ABFO94PYzonlkUsysSd+J7WDMyT6B/KwwAFACL7AQ8
4vK0TIB7yrWgaLsiDgAlADgzNzUtMjY5OS05OTIxLTkyNzgtMzA4My05MDQ1LTc5AA8AGgBNaWNyb3NvZnQgQ29ycG9yYXRpb24AEAAaAE1pY3Jvc29mdCBDb3Jwb3JhdGlvbgARABQAVmlydHVhbCBNYWNo
aW5lABIACQBOb25lABMAFABWaXJ0dWFsIE1hY2hpbmUAFwAeAEh5cGVyLVYgVUVGSSBSZWxlYXNlIHY0LjEAFAAaAE1pY3Jvc29mdCBDb3Jwb3JhdGlvbgAVABQAVmlydHVhbCBNYWNoaW5lABYAHgBIeXBl
ci1WIFVFRkkgUmVsZWFzZSB2NC4xABwAHwB8VmlydHVhbCBEaXNrICAgIHxNc2Z0ICAgIAAdABYAAAAAAAAAAAAAAAAAAAAAAAAAEBHgBGAE0AaQBjAHIAbwBzAG8AZgB0AHwATQBpAGMAcgBvAHMAbwBmAHQA
IABIAHkAcABlAHIALQBWACAAVgBpAGQAZQBvACUAMAAoAAAAKAAAAAEAAAABAAEAAQAAAAAAAQABAAAAonYGdqgtwrFk3rJ9hppeI0NTJABaeuhAEMx0MbNlwcHkbWf5k4zvKNV6KiSwkPByKsTZ3gAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

2. In the Microsoft Endpoint Manager admin center: https://endpoint.microsoft.com
   - Navigate to Devices > Windows > Windows enrollment > Devices
   - Click Import and upload the `AutopilotHWID.csv` file



Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.

Last successful sync
05/22/2025, 09:26 AM

Last sync request
05/22/2025, 09:26 AM

☐	Serial number	Manufacturer	Model	Group tag	Profile status	Purchase order	Userless Enrollment St...
☐	8375-2699-9921-9278-3083-9045-79	Microsoft Corporation	Virtual Machine		Assigned		Not Allowed

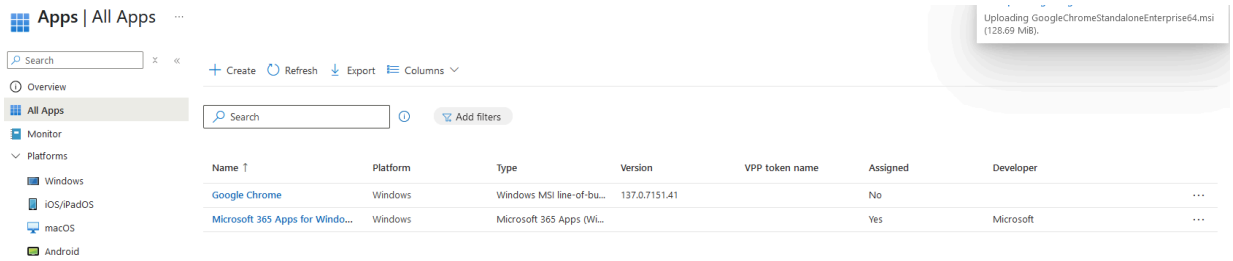
Step 4. Create an Autopilot Deployment Profile

1. In the Microsoft Endpoint Manager admin center:
   - Go to Devices > Windows > Windows enrollment > Deployment Profiles
   - Click Create profile > Windows PC
   - Configure the profile:
     - Name: e.g., "DipeshCorp - Standard Autopilot Profile"
     - Deployment mode: User-driven
     - Join to Microsoft Entra ID as: Microsoft Entra joined or Hybrid
     - Out-of-box experience (OOBE) settings:
     - Hide privacy settings

- Hide change account options
- User account type: Standard
- Language (Region): Operating System default
- Automatically configure keyboard: Yes
- Assign the profile to the "Windows Autopilot Devices" group

Step 5. Deploy Apps for Pre-configured Windows

1. In the Microsoft Endpoint Manager admin center:
    - Navigate to Apps > All Apps > + Create > Select Apps Type
        - Microsoft 365 Apps > Windows 10 and later
            - Skip App suit information
            - Configure app suite > Select Office apps
            - App suite information
                - Architecture: 64-bit
                - Default file format: Office Open Document Format
                - Update channel: Current Channel (Preview)
            - Assignments > Add Group > “Windows Autopilot Devices”
            - Review and Create
        - Same Process > Select “Line-of-business app”
            - Download “Google Standalone Stable Chrome”
            - Select app package file from Device > GoogleChromeStandaloneEnterprise64.msi
                - Publisher: Google
                - Category: Productivity
            - Assignments > Add Group > “Windows Autopilot Devices”
            - Review and Create



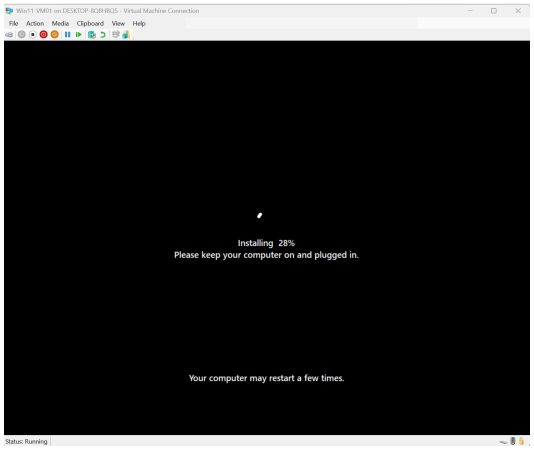
- Show app and profile configuration progress: Yes
- Block device use until all apps and profiles are installed: Yes
- Allow users to reset device if installation error occurs: No
- Assign the ESP to the "Windows Autopilot Devices" group

Step 6. Configure the Enrollment Status Page (ESP)

2. In the Microsoft Endpoint Manager admin center:
   - Navigate to Devices > Windows > Enrollment > Enrollment Status Page
   - Click Create
     - Name: Device Setup Status
     - Settings > Enabled “Show apps and profile configuration progress”
     - Assignments > Select “ Windows Autopilot Devices” Group
     - Review and Create

Step 7. Test the Autopilot Deployment

1. On a device registered for Autopilot:
   - Ensure it has an internet connection
   - Power on the device
   - The device will go through the OOBE, applying the Autopilot profile settings
   - The user will be prompted to sign in with their Microsoft Entra ID credentials



- The device will automatically enroll in Intune and apply assigned policies and applications

---

V. Completion Outcome:

At the end of this phase, DipeshCorp (*Alias of **nxhz***) successfully established Microsoft Intune as the Mobile Device Management (MDM) authority, enabling centralized management of corporate endpoints. A baseline security configuration profile was created and deployed to enforce essential device hardening policies. A Windows 11 virtual machine was manually enrolled into Intune, demonstrating successful device registration and policy assignment. The device's hardware hash was captured and uploaded to the Autopilot portal, and a user-driven deployment profile was configured and assigned. This marks the completion of a fully functional proof-of-concept for modern, cloud-first endpoint provisioning using Windows Autopilot.