Autopilot Intune Deployment Guide

This guide provides a comprehensive, step-by-step walkthrough for deploying Windows Autopilot with Microsoft Intune. It is designed for beginners and non-technical users, explaining each step, its purpose, and the consequences of skipping it.

Step 1: Preparation

Azure AD Join Configuration

Why: Devices must be registered in Azure Active Directory (Azure AD) to enable identity and access management. Without this, devices cannot authenticate to cloud resources, and enrollment will fail.

Configuration Steps:

1. 1. Go to Azure Portal → Azure Active Directory → Devices → Device Settings.
2. 2. Ensure 'Users may join devices to Azure AD' is set appropriately.
3. 3. Verify that device registration is enabled.

Intune Tenant Setup

Why: Microsoft Intune is the Mobile Device Management (MDM) platform used to apply policies and deploy apps. Without setting up Intune, devices cannot be managed.

Configuration Steps:

4. 1. Go to Microsoft Endpoint Manager Admin Center.
5. 2. Navigate to Tenant Administration → Connectors and Tokens → Microsoft Intune Enrollment.
6. 3. Verify MDM authority is set to Intune.

Licensing

Why: Autopilot and Intune features require valid licenses such as Microsoft 365 E3/E5 or Intune standalone. Without licensing, devices cannot be enrolled or managed.

Configuration Steps:

7. 1. Assign licenses to users via Microsoft 365 Admin Center.
8. 2. Ensure licenses include Intune and Azure AD Premium.

Windows Image Preparation

Why: A clean and standardized Windows image ensures consistent configuration and security. Skipping this may lead to performance issues and inconsistent user experience.

Configuration Steps:

9. 1. Use Windows Configuration Designer or MDT to create a custom image.
10. 2. Ensure the image includes latest updates and drivers.

Driver Package Import

Why: Importing hardware-specific drivers ensures devices function correctly. Missing drivers may cause boot failures or hardware malfunctions.

Configuration Steps:

11. 1. Download drivers from OEM website.
12. 2. Use MDT or Configuration Manager to inject drivers into the image.

Step 2: Device Enrollment

Device Import (CSV/Hardware Hash)

Why: Autopilot uses hardware hashes to identify devices. Without this, devices cannot be assigned profiles.

Configuration Steps:

13. 1. Export hardware hash using PowerShell script: Get-WindowsAutopilotInfo.ps1.
14. 2. Upload CSV file to Microsoft Endpoint Manager → Devices → Windows Autopilot Devices.

Autopilot Profile Creation

Why: Profiles define deployment mode and user experience. Without them, devices require manual setup.

Configuration Steps:

15. 1. Go to Endpoint Manager → Devices → Windows → Windows Enrollment → Deployment Profiles.
16. 2. Create a new profile and assign it to device group.

Enrollment Status Page (ESP)

Why: ESP ensures critical apps and policies are applied before user access. Skipping this may expose devices to risks.

Configuration Steps:

17. 1. Navigate to Endpoint Manager → Devices → Windows → Enrollment Status Page.
18. 2. Create and assign ESP to Autopilot devices.

Network Connectivity

Why: Devices need internet access to contact Azure AD and Intune. Without it, enrollment fails.

Configuration Steps:

19. 1. Ensure devices are connected to a network during OOBE.
20. 2. Verify firewall and proxy settings allow access to Microsoft services.

Step 3: Configuration & Deployment

App Deployment

Why: Ensures business apps are installed automatically. Skipping this reduces productivity.

Configuration Steps:

21. 1. Go to Endpoint Manager → Apps → Add.
22. 2. Choose app type (Win32, MSI) and configure deployment settings.

Configuration Profiles

Why: Applies security settings and compliance rules. Without them, devices may be non-compliant.

Configuration Steps:

23. 1. Navigate to Endpoint Manager → Devices → Configuration Profiles.
24. 2. Create profiles for device restrictions, Wi-Fi, VPN, etc.

Security Baselines

Why: Enforces Microsoft-recommended security configurations. Skipping this increases vulnerability.

Configuration Steps:

25. 1. Go to Endpoint Manager → Endpoint Security → Security Baselines.
26. 2. Assign baselines to device groups.

Update Rings

Why: Controls Windows Update rollout. Without it, updates may cause downtime.

Configuration Steps:

27. 1. Navigate to Endpoint Manager → Devices → Update Rings.
28. 2. Create pilot and production rings with appropriate settings.

Targeted Device Groups

Why: Enables policy and app assignment. Incorrect targeting leads to misconfiguration.

Configuration Steps:

29. 1. Create dynamic/static groups in Azure AD.
30. 2. Assign policies and apps to these groups.

Step 4: Advanced Enhancements

Hybrid Azure AD Join

Why: Supports organizations with on-prem AD. Without it, legacy systems may not integrate.

Configuration Steps:

31. 1. Configure Azure AD Connect with Hybrid Join settings.
32. 2. Verify device registration in both on-prem and cloud directories.

Conditional Access

Why: Enforces MFA and Zero Trust. Skipping this may allow unauthorized access.

Configuration Steps:

33. 1. Go to Azure AD → Security → Conditional Access.
34. 2. Create policies for MFA, location-based access, and app restrictions.

Role-Based Access Control (RBAC)

Why: Secures admin operations. Without RBAC, users may have excessive privileges.

Configuration Steps:

35. 1. Navigate to Endpoint Manager → Tenant Administration → Roles.
36. 2. Create custom roles and assign to users/groups.

Monitoring & Reporting

Why: Tracks compliance and deployment status. Without it, issues may go unnoticed.

Configuration Steps:

37. 1. Use Endpoint Manager dashboards.
38. 2. Generate reports for device compliance, app status, and enrollment.

Step 5: Troubleshooting

Common issues and resolutions:

Issue: Enrollment fails

Solution: Check network connectivity, licensing, and profile assignment.

Issue: Apps not installing

Solution: Verify app deployment settings and ESP configuration.

Issue: Device not appearing in Intune

Solution: Ensure hardware hash is uploaded and synced.

Issue: Security baselines not applying

Solution: Check group assignment and baseline version compatibility.

Microsoft Official References

Windows Autopilot Overview: https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot

Intune Documentation: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Azure AD Join: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join

Conditional Access: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Scenario: Remote Employee Deployment
A company ships laptops directly to remote employees. Autopilot ensures devices are pre-configured and secure. Skipping ESP could allow access before security policies are applied.

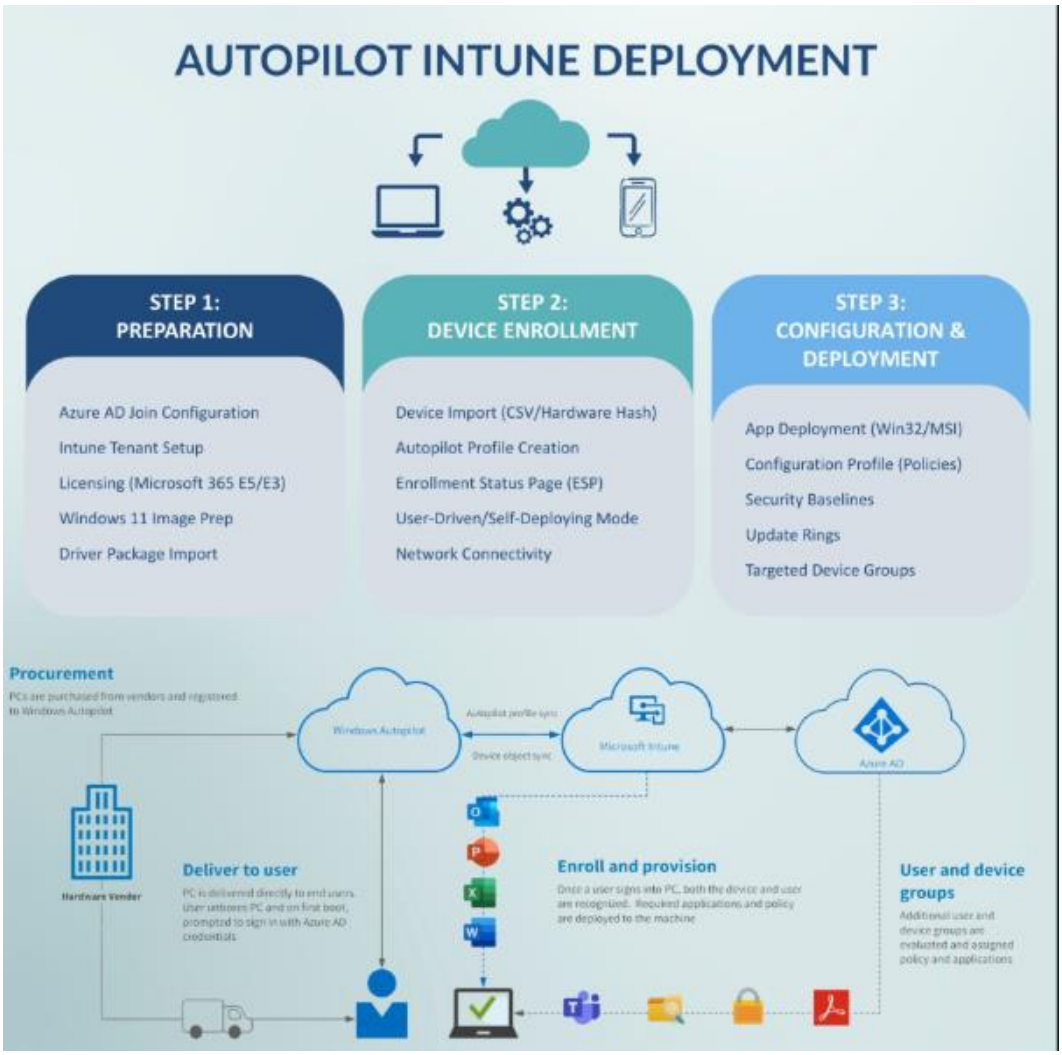
Scenario: Hybrid Azure AD Join
An enterprise with on-prem AD uses Hybrid Join to maintain legacy identity systems while enabling cloud management. Missing this setup causes sync failures.

Scenario: Conditional Access Enforcement
A user tries to access corporate resources from an unmanaged device. Conditional Access blocks access until device compliance is verified.

Scenario: Intune Policy Assignment
Sales team devices receive different apps and policies than

engineering. Without proper targeting, users may lack necessary tools or face security risks.

Visual Diagrams and Flowcharts



Autopilot Workflow Diagram

Real-World Scenarios with Solutions

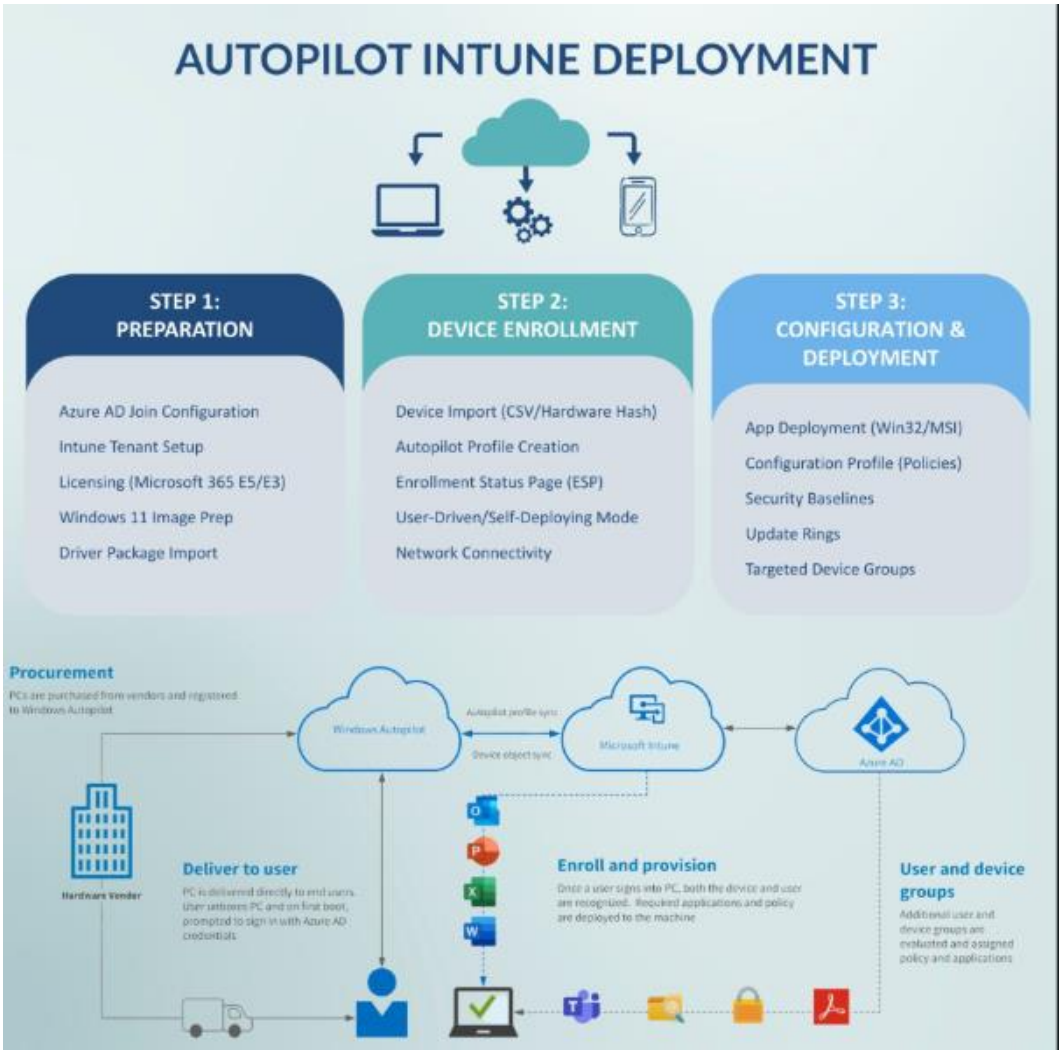
Scenario: Remote Employee Deployment
Problem: Devices shipped to remote employees may be accessed before security policies are applied.
Solution:
1. Enable ESP in Intune.
2. Assign required apps and policies.
3. Test deployment using OOBE simulation.

Scenario: Hybrid Azure AD Join
Problem: Sync failures due to missing Hybrid Join setup.
Solution:
1. Install Azure AD Connect.
2. Configure Hybrid Join in the wizard.
3. Verify sync status in Azure AD → Devices.

Scenario: Conditional Access Enforcement
Problem: Unmanaged devices accessing corporate resources.
Solution:
1. Create Conditional Access policy in Azure AD.
2. Set conditions to require compliant device.
3. Test login from unmanaged device.

Scenario: Intune Policy Assignment
Problem: Incorrect app/policy targeting for departments.
Solution:
1. Create dynamic groups in Azure AD.
2. Assign apps and policies to respective groups.
3. Verify deployment in Endpoint Manager.

Deployment Summary and Quick Reference



Deployment Flowchart Summary

Quick Reference Checklist:
✓ Azure AD Join configured
✓ Intune tenant setup
✓ Licenses assigned
✓ Windows image and drivers prepared
✓ Devices imported via hardware hash
✓ Autopilot profiles created
✓ ESP configured
✓ Apps and policies assigned
✓ Security baselines applied
✓ Update rings configured
✓ Device groups targeted
✓ Hybrid Join (if needed)

✓ Conditional Access policies enforced
✓ RBAC roles assigned
✓ Monitoring and reporting enabled