Project Title:
Microsoft Intune Autopilot Deployment & Implementation

Contact Information:
Professor AJ Lapid < AllanJames.Lapid@brooklyn.cuny.edu
CC: Professor Chuang < chuang@sci.brooklyn.cuny.edu

Supervisor:
Pierre Polycarpe

Abstract:
This project presents a detailed plan for deploying Microsoft Intune Autopilot, followed by the implementation of several Intune features aimed at improving device management, security, and operational efficiency within an organization. The main goal is to automate the provisioning of new devices via Autopilot, streamlining setup and pre-configuration, and then integrating key features like Windows Update Management, Endpoint Analytics, BitLocker Management, and Office 365 deployment. The project is structured into distinct phases: initiation, planning, preparation, deployment, post-deployment configuration, testing, and closure. Each phase includes specific deliverables.

The key tasks involve setting up the environment for Autopilot, deploying and configuring devices, implementing essential Intune features, testing the configurations, and creating use cases to support the technician's implementation.

The success of the project will be determined by the seamless deployment of Intune Autopilot, the timely completion of all features, high user satisfaction, and the avoidance of security incidents. Ultimately, the project aims to improve the organization’s device management capabilities, strengthen security, and create a smooth experience for IT teams and users.

Tools and list of components:
The project's software components include Microsoft Intune, a cloud-based device management platform, and Microsoft Autopilot, a Windows device deployment service. The most recent versions of Microsoft Endpoint Configuration Manager and Office 365 Suite will also be used. Devices will run the most recent versions of Windows 10 or 11 Enterprise, with BitLocker used for encryption management. Endpoint Analytics will be used to monitor device performance, with Azure Active Directory (latest version) handling identity and access control.

The Hardware will include Windows laptops and desktops for deployment testing.

Role-based access control (RBAC) with Microsoft Intune

To configure Intune and set up Autopilot deployment, you'll need to assign the Intune Administrator role. While other roles are available, it's best to assign the role with the least permissions necessary for security reasons.

Diagrams/designs and plans for the technical implementation

Azure contains over 100 services to assist you with various cloud computing scenarios and possibilities. Microsoft Intune is one of several services available in Azure. Intune helps you ensure that your company's devices, apps, and data meet your company's security requirements. You have the control to set which requirements need to be checked and what happens when those requirements aren't met. The Azure portal is where you can find the Microsoft Intune service. Understanding the features available in Intune will help you accomplish various Mobile Device Management (MDM) and Mobile Application Management (MAM) tasks.

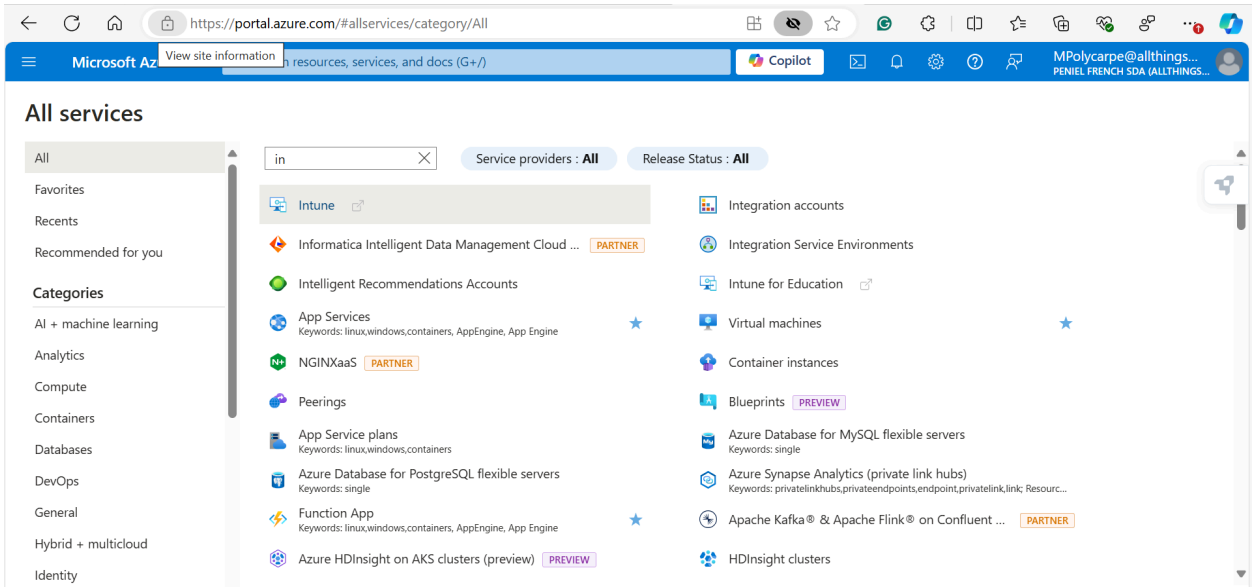


Figure 1. Microsoft Intune

Technical implementations

For the technical implementation of the Microsoft Intune Autopilot project, multiple diagrams and designs will help visualize the overall process, including system architecture, workflows, and key components.

1. System Architecture Diagram

This diagram illustrates the overall architecture of the project, showing how different components, such as Microsoft Intune, Azure Active Directory (AAD), Microsoft Autopilot, and Endpoint Analytics, interact with each other.

- **Key Components:**
    - Devices (laptops/desktops)
    - Microsoft Intune (Cloud-based device management)
    - Azure Active Directory (Identity and access management)
    - Microsoft Endpoint Configuration Manager

This design ensures that every device communicates with the cloud services (Intune, AAD) to receive configuration and management policies, ensuring proper security and deployment automation.

Licensing requirements:

To use Intune Autopilot, you need the appropriate licensing. The licensing requirements typically include:

1. Microsoft Intune License:

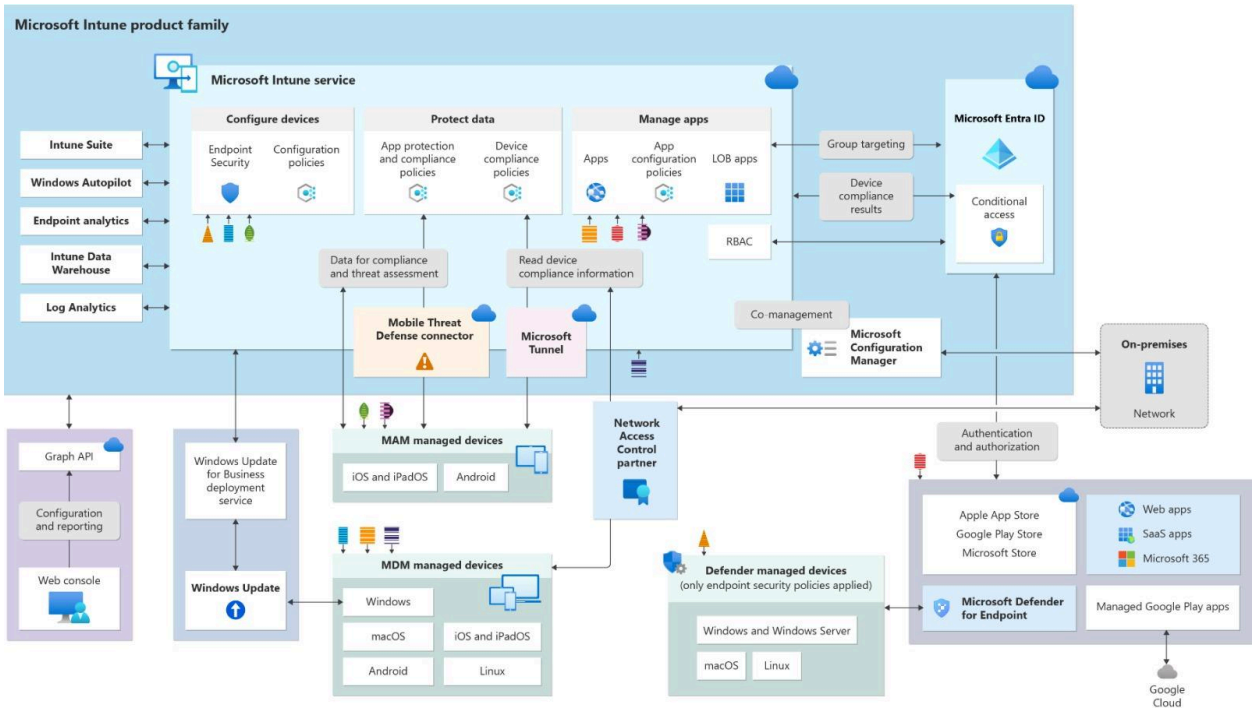
Autopilot requires an active Intune license. Intune is part of the Microsoft 365 suite, so any plan that includes Intune, such as Microsoft 365 Business Premium, Microsoft 365 E3, or Microsoft 365 E5, will suffice. For this project, we will be using Microsoft 365 E5 license.

2. Windows 10/11 Pro, Enterprise, or Education:

Devices being set up with Autopilot need to be running Windows 10 Pro, Enterprise, or Education, or Windows 11 Pro, Enterprise, or Education. Windows Home editions are not supported.

For Intune Autopilot, the OS versions that are compatible are:

1. **Windows 10**: Versions 1809 and later are supported. However, for the best experience, it's recommended to use the latest version of Windows 10.
2. **Windows 11**: All versions of Windows 11 are supported. As with Windows 10, using the latest version is recommended to benefit from the latest features and security updates.



Note: On-premises network will not be used in this project.

Figure 2. Microsoft Intune Product Family

2. Deployment Workflow Diagram

The workflow diagram describes the step-by-step process involved in the automated provisioning of new Windows devices through Microsoft Autopilot. It shows the user interaction with the device during setup and how the Autopilot service kicks in to apply policies and configurations.

- **Stages:**
    1. Customers purchase hardware from a vendor
    2. Vendor fulfill and ship device to end user
    3. The user powers on the device connect to the internet, and signs in with organizational credentials.
    4. Intune Autopilot automatically enrolls and configures the device based on predefined organizational policies (security, software deployment, etc.).
    5. The device is ready for use with full security and compliance.

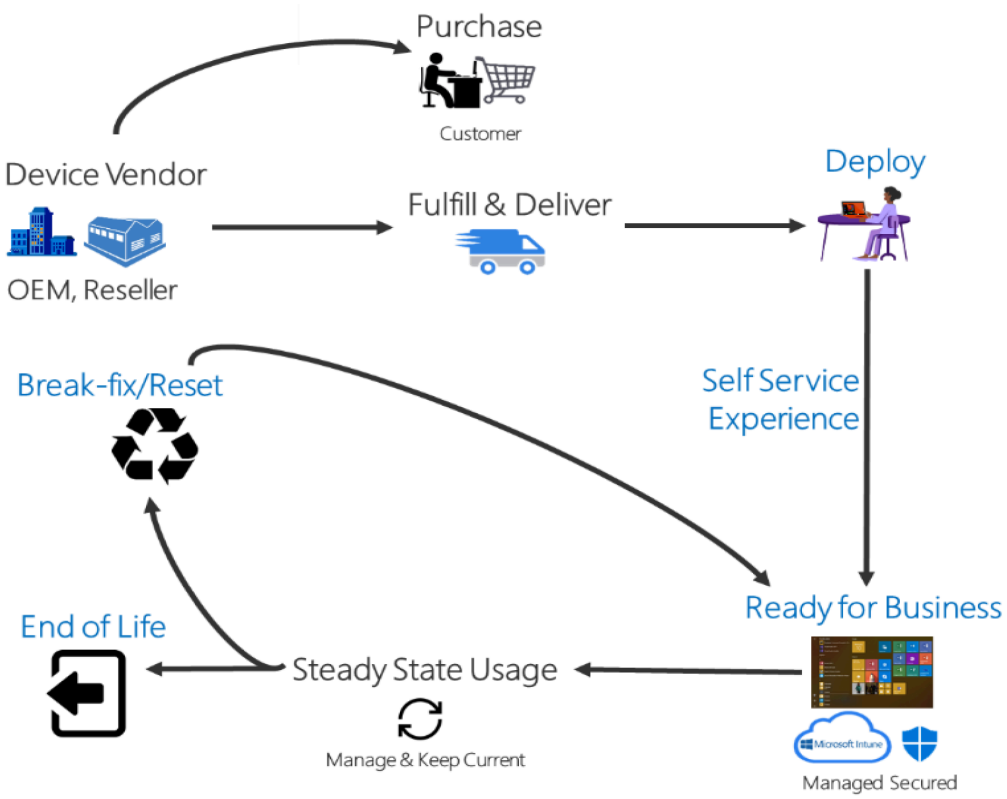


Figure 3. Windows Autopilot

3. Security Compliance Diagram

This diagram focuses on security enforcement, showing how BitLocker encryption and other security policies are applied during and after device enrollment. The diagram outlines how devices receive encryption policies, apply BitLocker, and store recovery keys securely.

- **Key Steps:**
    1. Device enrollment in Intune.
    2. Application of security compliance policies.
    3. Activation of BitLocker encryption.
    4. Data encryption status report sent back to Intune.

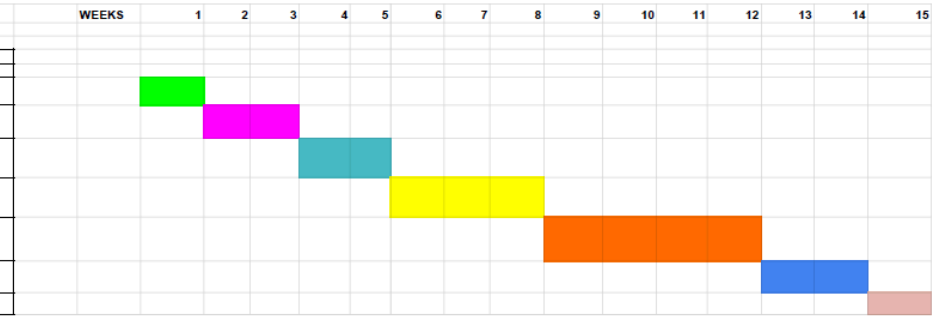
This diagram ensures that device encryption and security measures are enforced consistently across the organization's network.

Project Tentative Schedule

Phase	Description	Timeline Duration	Responsible Party
Initiation	Define project scope, objectives, stakeholders, and resources.	1week(Week 1)	Project manager
Planning	Develop project plan, risk management, and communication strategy.	2weeks(Week 2 & 3)	Project manager
Preparation	Configure network settings and security policies for Autopilot deployment.	2weeks(Week 4 & 5)	IT Admin, Security Team
Deployment	Deploy Intune Autopilot and ensure the configuration of devices.	3weeks(Week 6, 7, 8)	IT Admin
Post-Deployment Configuration	Implement additional Intune features like Windows Update Management and Endpoint Analytics.	4 weeks (Week 9, 10, 11, 12)	IT Admin, Security Team, Project Team
Testing and Validation	Test and validate all features and configurations.	2 weeks(Week 13, 14)	QA Team, IT Admin
End of project	Review project outcomes and close the project.	1 week (Week 15)	Project manager

Project Tentative Schedule

PHASE	DESCRIPTION	TIMELINE	RESPONSIBLE PARTY
Initiation	Define project scope, objectives, stakeholders, and resources.	1 week	Project Manager
Planning	Develop project plan, risk management, and communication strategy.	2 weeks	Project Manager
Preparation	Configure network settings and security policies for Autopilot deployment.	2 weeks	IT Admin, Security Team
Deployment	Deploy Intune Autopilot and ensure the configuration of devices.	3 weeks	IT Admin
Post-Deployment Configuration	Implement additional Intune features like Windows Update Management and Endpoint Analytics.	4 weeks	IT Admin, Security Team, Project Team
Testing and Validation	Test and validate all features and configurations.	2 weeks	QA Team, IT Admin
Closure	Review project outcomes and close the project.	1 week	Project Manager



Data Sources:

I will probably employ a variety of datasets and data sources for a Microsoft Intune Autopilot deployment and implementation project with a primary focus on device configuration and administration. The primary datasets and data sources that you would usually come across are listed below:

- Azure Active Directory: For user identity and device authentication.
- Intune Device Management: For managing enrolled devices.
- Endpoint Analytics Data: To gather performance metrics of deployed devices.

Use Cases:

These use cases highlight the key scenarios where the system will be applied, demonstrating automation, security enforcement, and efficient device management through the Intune platform.

For use case purposes, there are different ways to configure autopilot deployment. Therefore, we will use the **user-driven method**. Please refer to the Windows 10 Autopilot deployment process.

1. Automated Device Provisioning:
    - Input: New Windows 10/11 devices are shipped to users. They connect to the internet and enter their credentials.
    - Process: Microsoft Intune Autopilot automatically configures the device based on pre-configured policies.
    - Output: The device is fully set up with security policies, Office 365 installed, and ready for use.
2. Security Compliance with BitLocker:

- Input: The device is enrolled into Intune, and a security compliance policy is applied.
- Process: BitLocker encryption is automatically applied to the device.
- Output: Device data is encrypted, ensuring compliance with organizational security policies.

3. Endpoint Analytics and Windows Update Management:
   - Input: Devices regularly report performance data and update status.
   - Process: Endpoint Analytics gathers data, and Windows Update Management ensures devices are updated based on organization settings.
   - Output: IT administrators can view reports, manage updates, and address issues remotely.

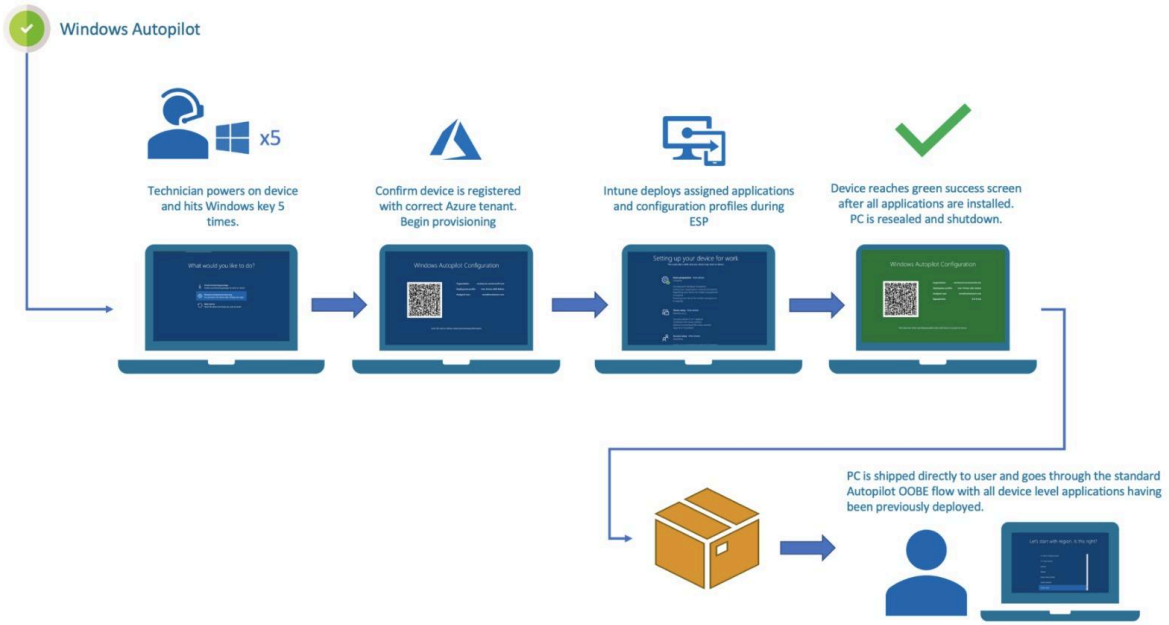


Figure 4. Windows Autopilot

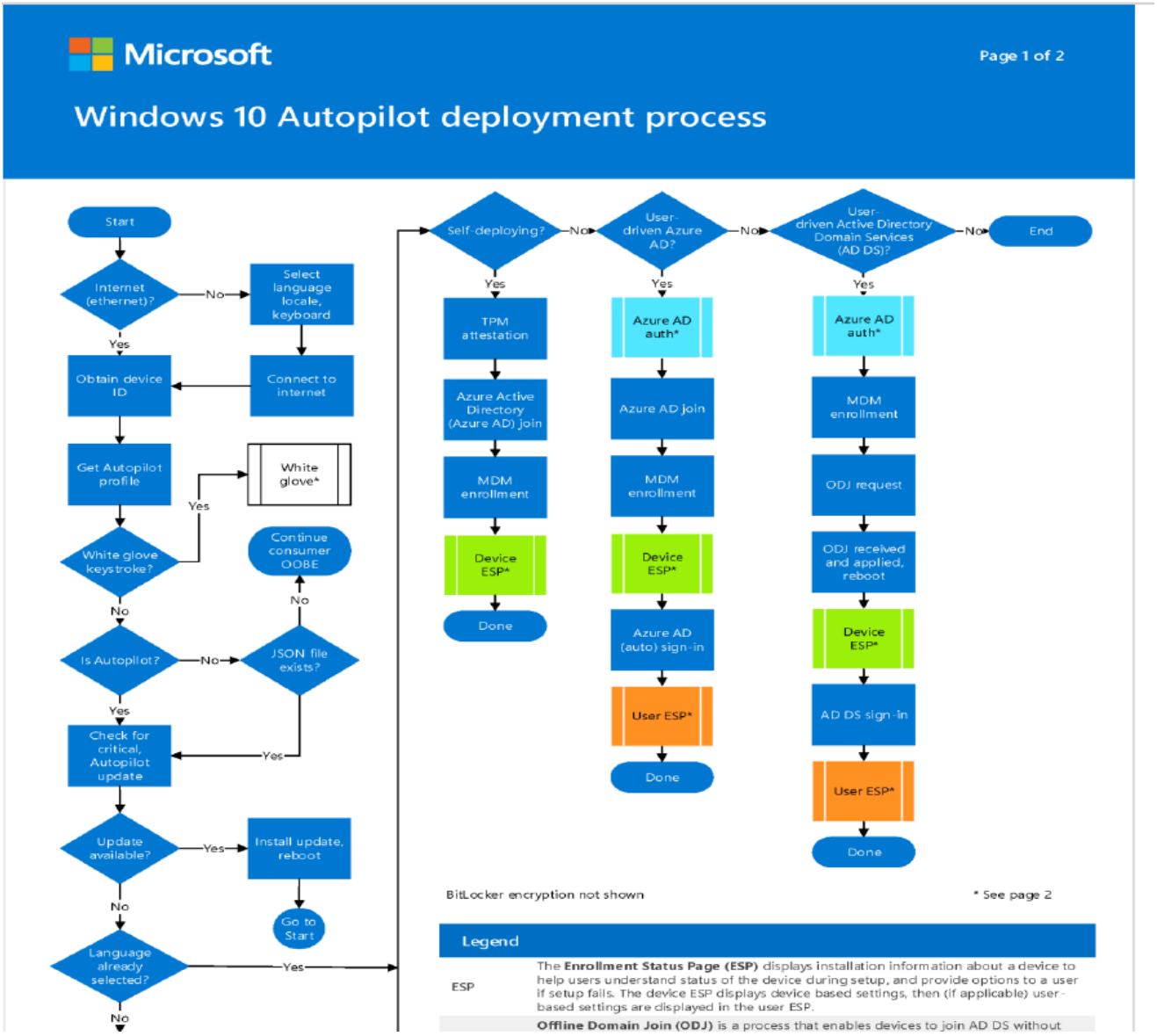


Figure 5. Windows 10 Autopilot Deployment Process