Microsoft Intune Autopilot Deployment & Implementation

Agenda

Team and Roles

Project Evolution/ What I've done so far

- Windows Autopilot Deployment Process
- Windows Autopilot Requirements
- Configuration Steps
- Security Features
- Dynamic Group and Profile Creation

Learning and Challenges

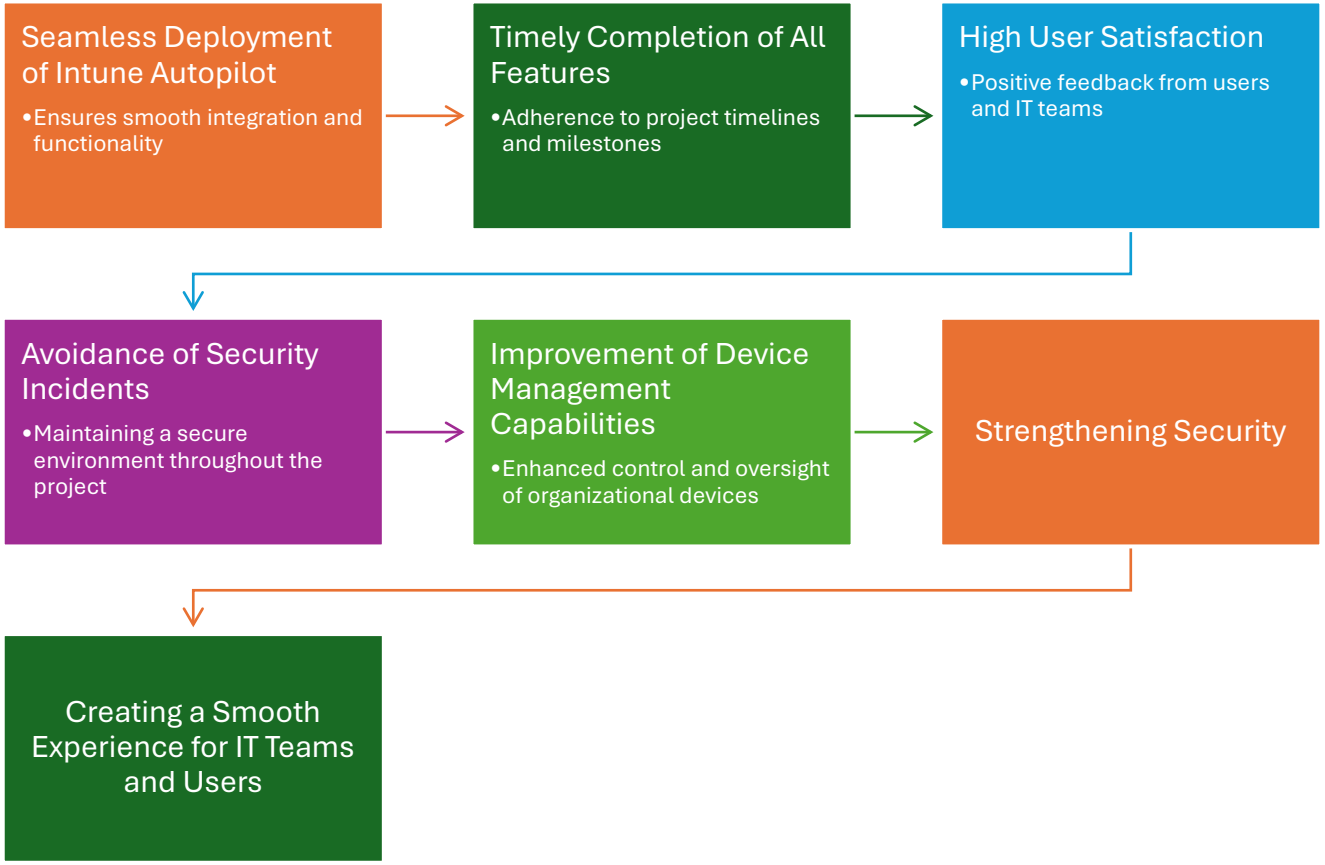
Abandoned and excited features

Toughest bug or interaction

Project Overview

- Project Overview
  - Deploy Microsoft Intune Autopilot
  - Implement Intune features for device management
- Main Goals
  - Automate provisioning of new devices
  - Streamline setup and pre-configuration
- Key Features
  - Windows Update Management
  - Endpoint Analytics
  - BitLocker Management
  - Office 365 deployment
- Project Phases

Project Success Criteria



Solo Project Responsibilities

Multiple Roles and Responsibilities

Act as team leader, project manager, developer, and technical specialist

Deep involvement in all role specialties

Comprehensive Project Management

Planning and research

Hands-on technical implementation and troubleshooting

Self-Reliance and Decision Making

Reading documentation and researching best practices

Resolving technical challenges independently

Ensuring Project Alignment

Managing overall progress

Aligning project with initial goals and objectives

Key Benefits of Windows Autopilot

Traditional IT Admin Tasks

- Maintaining various versions of custom Windows images
- Managing drivers for every device model

Windows Autopilot Advantages

- Uses OEM-optimized Windows 10/11
- Leverages existing Windows installation
- Makes devices ‘business-ready’ without reimaging

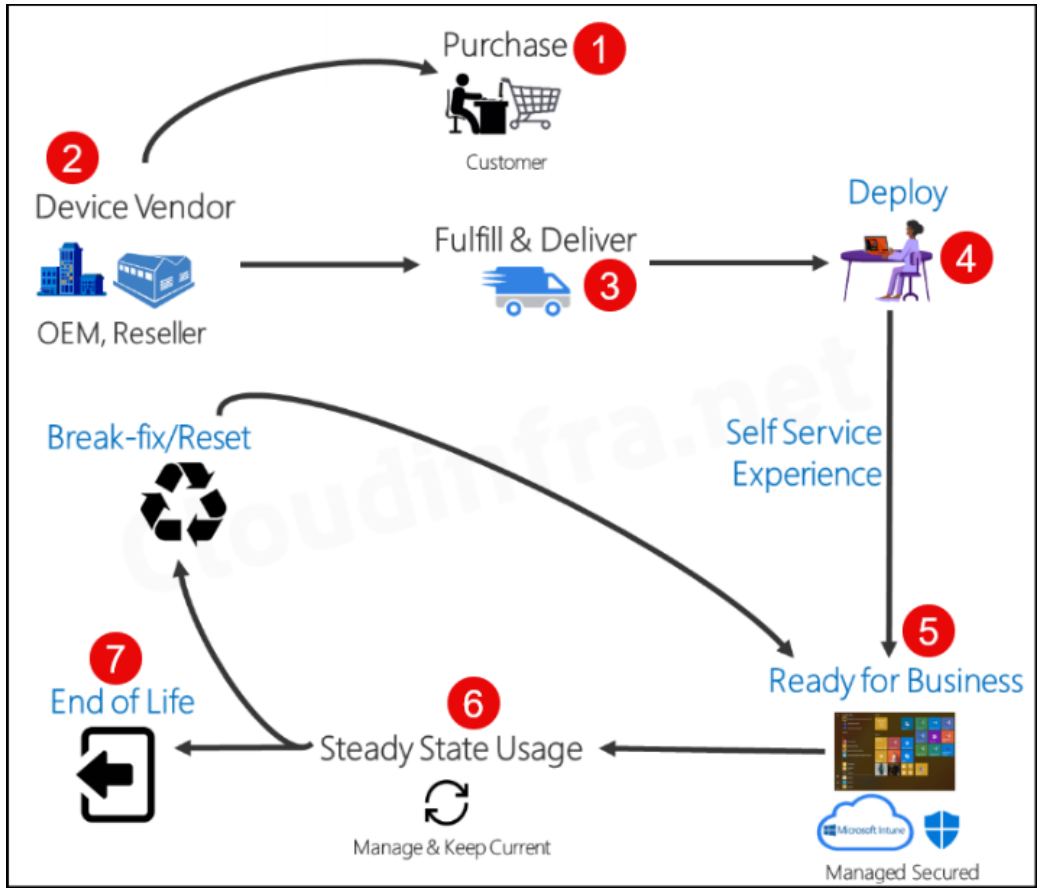
Autopilot Deployment Process

- Purchase: Customer/Organization buys the laptop
- Shipment: Device vendor, OEM, or reseller ships the laptop
- Delivery: Laptop is delivered to the end user

Resetting the Laptop

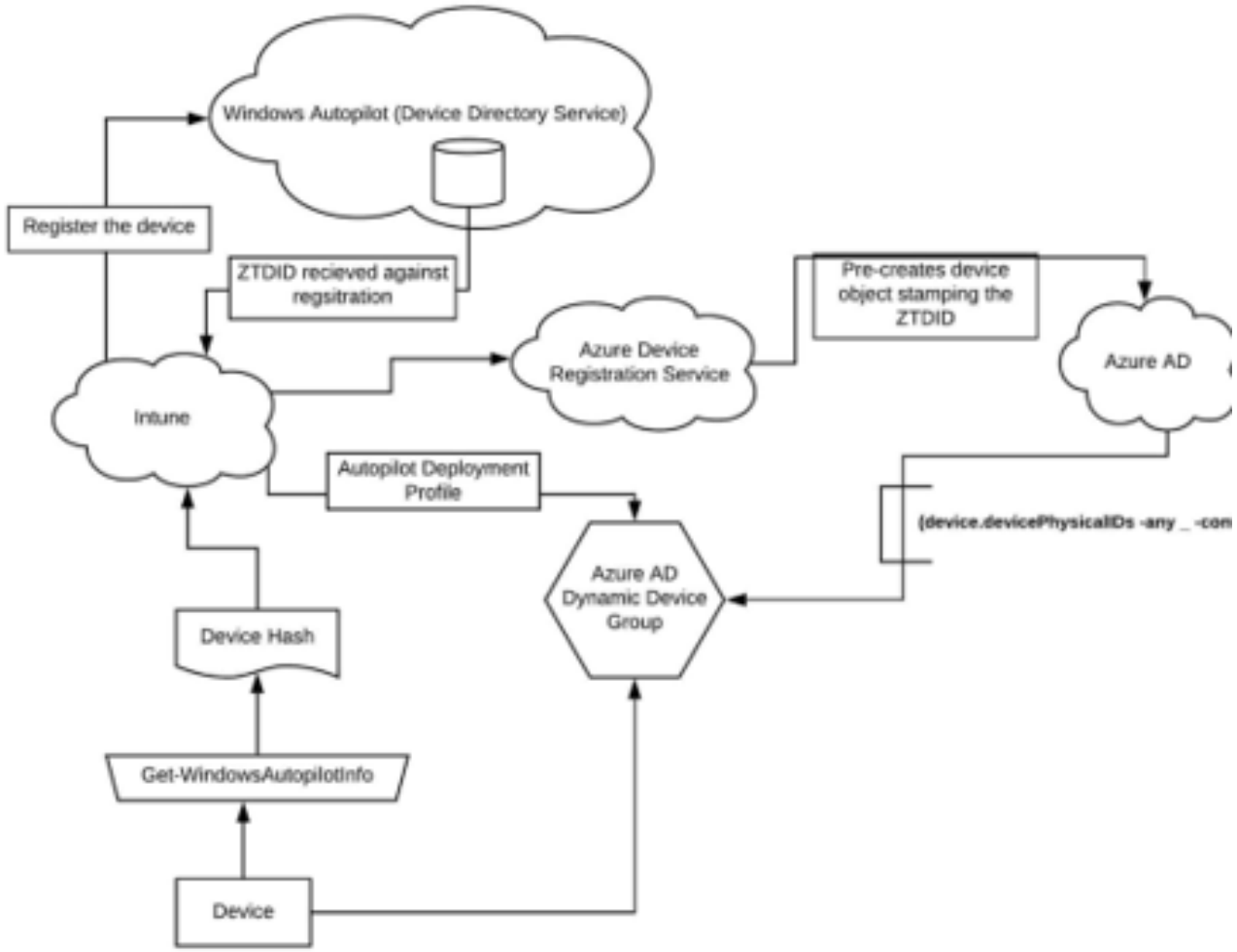
Windows Autopilot Overview

The sketch on the right illustrates the starting point of the Windows Autopilot deployment process and serves as a visual aid to help you better understand how Autopilot works.



High-level Architecture

- Windows Autopilot Design Overview
- This reference architecture shows how we will implement Autopilot to integrate with Microsoft Intune in Azure environment with Microsoft Entra ID

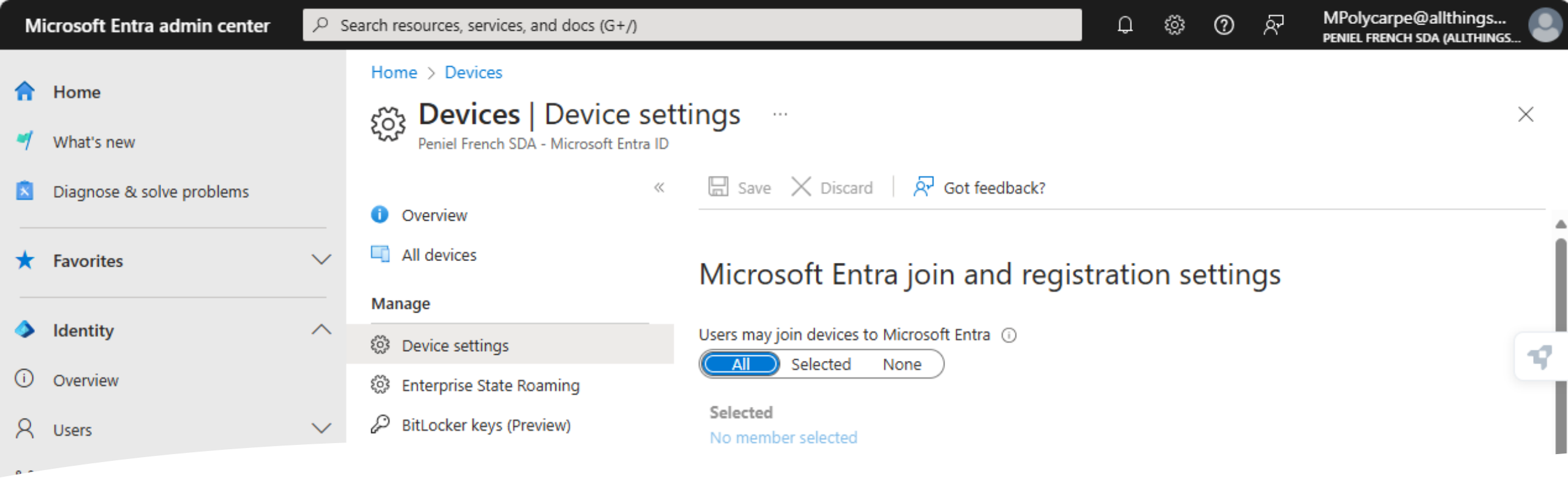


Supported Versions/Licensing

Platform	Supported Editions
Windows 11	Windows 11 Pro Windows 11 Pro Education Windows 11 Pro for Workstations Windows 11 Enterprise Windows 11 Education
Windows 10	Windows 10 Pro Windows 10 Pro Education Windows 10 Pro for Workstations Windows 10 Enterprise Windows 10 Education

Required Subscriptions for Windows Autopilot

Microsoft 365 Business Premium
Microsoft 365 F1 or F3
Microsoft 365 Academic A1, A3, or A5
Microsoft 365 Enterprise E3 or E5
Enterprise Mobility + Security E3 or E5
Intune for Education
Microsoft Entra ID P1 or P2 and Microsoft Intune



Allow Users to Join Devices to Entra ID

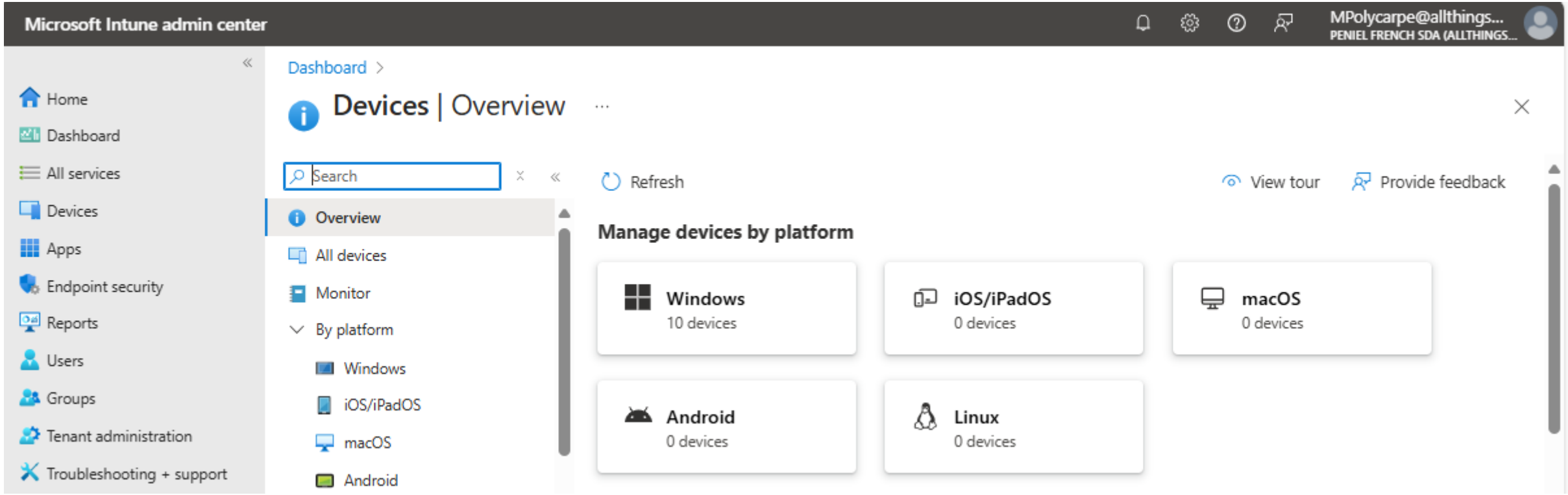
- Importance of Joining Devices to Entra ID
  - Critical for device enrollment in Intune
  - Ensures proper device management
- Options for Allowing Users
  - Select All: All users can join devices
  - Selected: Use existing Entra security groups

Enable Automatic Enrollment

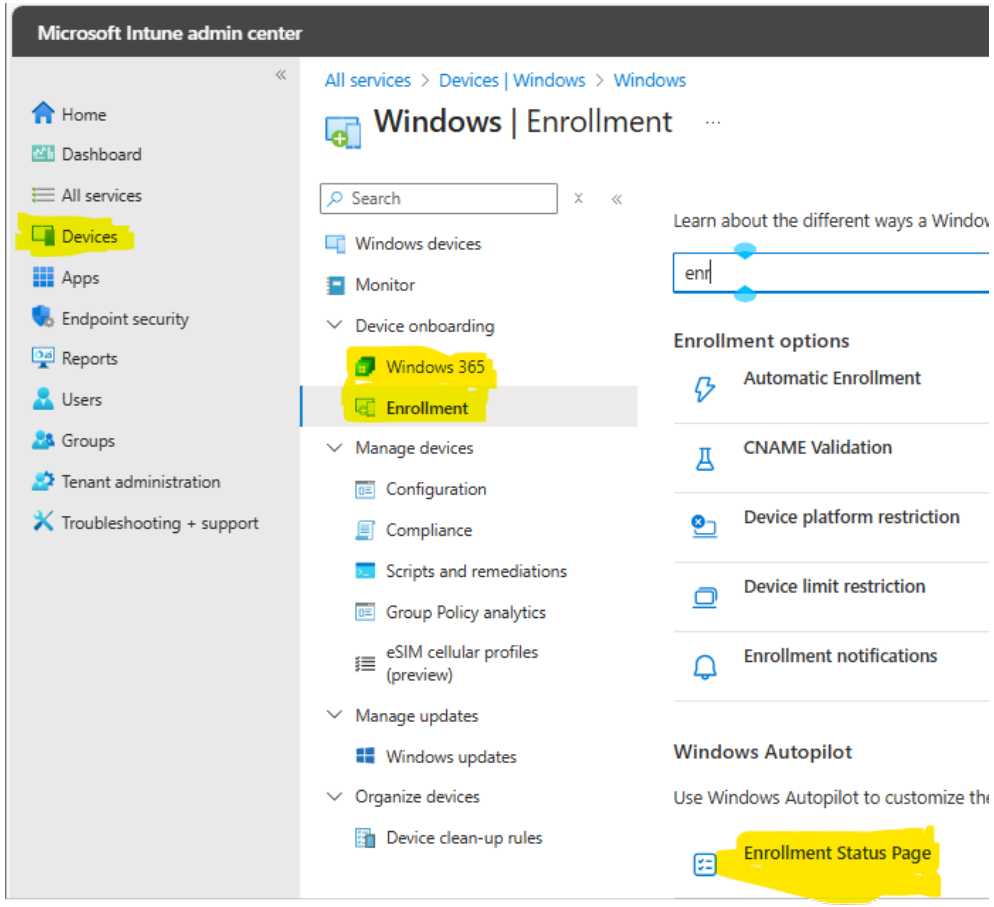
Device Enrollment Process
- Device joins Entra ID
- Automatic Enrollment enabled
- Device enrolls in Intune

Configuration Steps
- Set MDM user scope to All
- Set Windows Information Protection (WIP) user scope to None

Project Success Criteria
- Seamless deployment of Intune Autopilot
- Timely completion of all features
- High user satisfaction



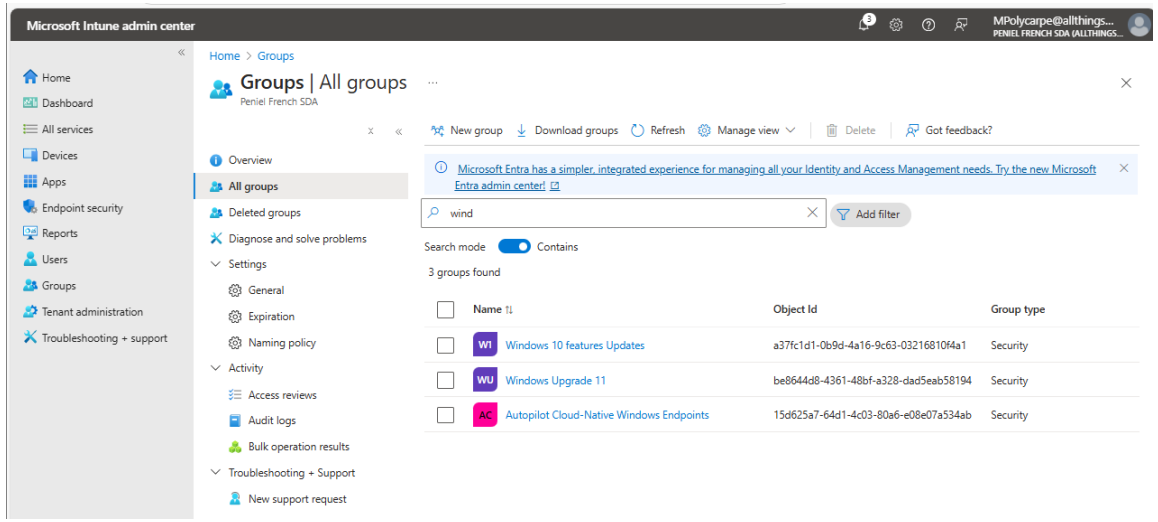
Setup Enrollment Status Page (ESP)



Enrollment Status Page (ESP) Overview	ESP Configuration in Microsoft Intune Admin Center	ESP Functionality in Windows Autopilot	Benefits of ESP
•Appears during initial device setup and first user sign-in •Shows configuration progress of assigned apps and profiles	•Manages end-user experience during device provisioning •Highlights two ESP profiles: Windows Autopilot and All Users and All Devices	•Ensures devices are fully configured and compliant before user access •Monitors app installation, profile configuration, and policy assignments •Provides real-time updates throughout the setup process	•Streamlines deployment

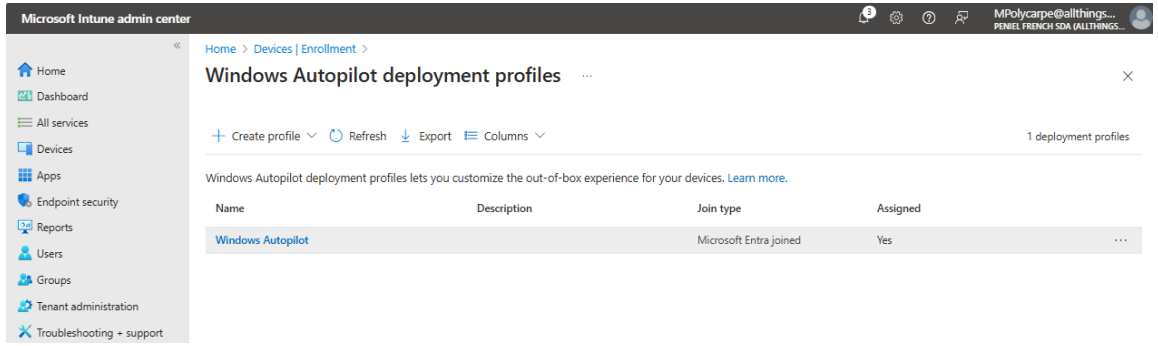
Create Microsoft Entra Dynamic Group

- Created a Dynamic Microsoft Entra Group
  - Automatically includes devices imported to Windows Autopilot
  - Used Group Tag Cloud Native
- Target Configurations and Applications
  - Apply settings to the dynamic group
- Note on Dynamic Groups
  - Groups take a few minutes to populate
  - Longer wait times in large organizations
  - Confirm device membership after a few minutes

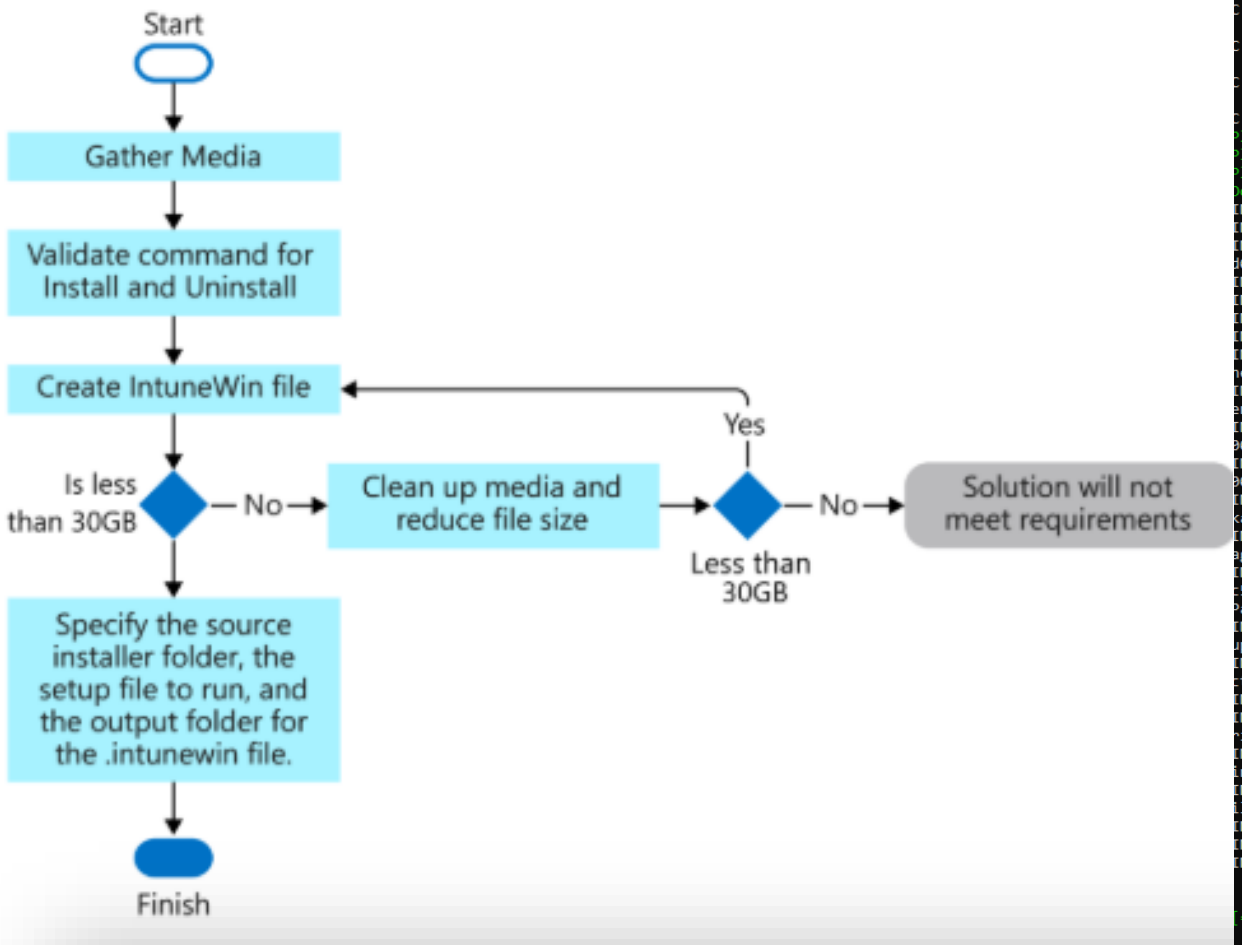


Created and Assigned the Windows Autopilot Profile

- Purpose of Windows Autopilot Profile
  - Automates the setup of new Windows devices
  - Reduces manual configuration
  - Specifies key settings like policies, apps, and configurations
- Configuration in Microsoft Intune
  - Manages how Windows devices are set up during OOBE
  - Defines how devices join Microsoft Entra ID
  - Applies settings or policies automatically
- Assignment to Microsoft Entra Group
  - Assigned to a test group called "Autopilot Cloud-Native Windows Endpoint"
  - Devices in this group automatically apply profile settings during OOBE
  - Ensures devices are business-ready with minimal user intervention



Process flow to create a .intunewin file



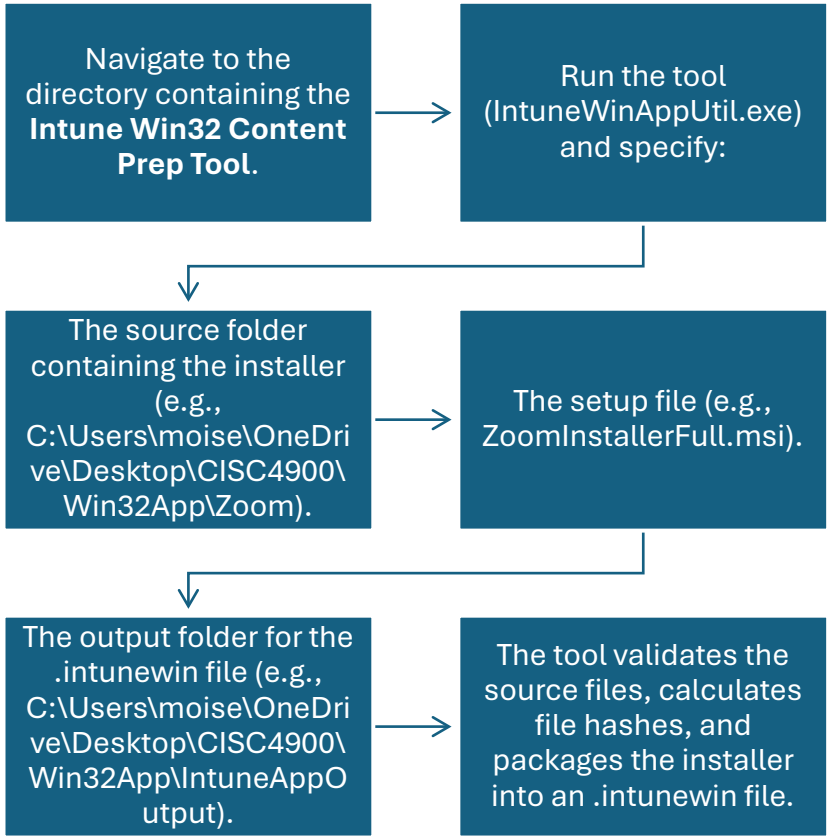

```
C:\Windows>cd..

C:\>cd Users

C:\Users>cd moise

C:\Users\moise>cd OneDrive

C:\Users\moise\OneDrive>cd Desktop

C:\Users\moise\OneDrive\Desktop>cd CISC4900

C:\Users\moise\OneDrive\Desktop\CISC4900>cd IntuneApps

C:\Users\moise\OneDrive\Desktop\CISC4900\IntuneApps>IntuneWinAppUtil.exe
Please specify the source folder: C:\Users\moise\OneDrive\Desktop\CISC4900\IntuneApps\7Zip
Please specify the setup file: 7z2408-x64.exe
Please specify the output folder: C:\Users\moise\OneDrive\Desktop\CISC4900\IntuneApps\7Zipintune
Do you want to specify catalog folder (Y/N)?N
INFO   Validating parameters
INFO   Validated parameters within 26 milliseconds
INFO   Compressing the source folder 'C:\Users\moise\OneDrive\Desktop\CISC4900\IntuneApps\7Zip' to 'C:\Users\moise\AppData\Local\Temp\f9e2e
d0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   Calculated size for folder 'C:\Users\moise\OneDrive\Desktop\CISC4900\IntuneApps\7Zip' is 1624144 within 2 milliseconds
INFO   Compressed folder 'C:\Users\moise\OneDrive\Desktop\CISC4900\IntuneApps\7Zip' successfully within 146 milliseconds
INFO   Checking file type
INFO   Checked file type within 16 milliseconds
INFO   Encrypting file 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\IntunePackage.intu
newin'
INFO   'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\IntunePackage.intunewin' has been
encrypted successfully within 66 milliseconds
INFO   Computing SHA256 hash for C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\26e864c5-
0008-41e7-9587-6c3bd4f8d521
INFO   Computed SHA256 hash for 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\26e864c5-
0008-41e7-9587-6c3bd4f8d521' within 25 milliseconds
INFO   Computing SHA256 hash for C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\IntunePac
kage.intunewin
INFO   Computed SHA256 hash for C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\IntunePack
age.intunewin within 33 milliseconds
INFO   Copying encrypted file from 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\26e864
c5-0008-41e7-9587-6c3bd4f8d521' to 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\Intune
Package.intunewin'
INFO   File 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Contents\IntunePackage.intunewin' got
updated successfully within 19 milliseconds
INFO   Generating detection XML file 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage\Metadata\Dete
ction.xml'
INFO   Generated detection XML file within 137 milliseconds
INFO   Compressing folder 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage' to 'C:\Users\moise\OneD
rive\Desktop\CISC4900\IntuneApps\7Zipintune\7z2408-x64.intunewin'
INFO   Calculated size for folder 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage' is 1610693 with
in 0 milliseconds
INFO   Compressed folder 'C:\Users\moise\AppData\Local\Temp\f9e2ed0e-07a5-42fa-8f24-4884a3b59f04\IntuneWinPackage' successfully within 88 m
illiseconds
INFO   Removing temporary files
INFO   Removed temporary files within 8 milliseconds
INFO   File 'C:\Users\moise\OneDrive\Desktop\CISC4900\IntuneApps\7Zipintune\7z2408-x64.intunewin' has been generated successfully


[==========]  100%                                                    INFO   Done!!!
```

Process Flow of Win32App

A Win32 application is a software program designed to run on the Microsoft Windows operating system, utilizing the Win32 Application Programming Interface (API) to access system functions and create a user interface, essentially referring to traditional desktop applications built for Windows, whether 32-bit or 64-bit; the "Win32" part signifies the programming interface used to develop these applications on Windows systems.

Summary Flow of Win32App

Command Prompt Workflow



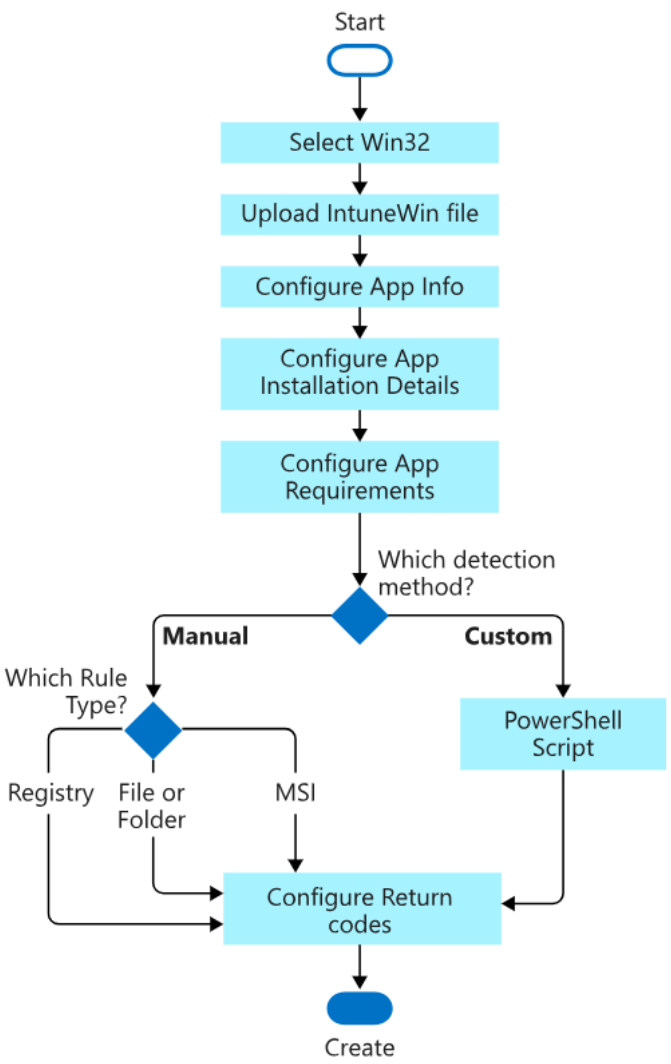
Process Flow

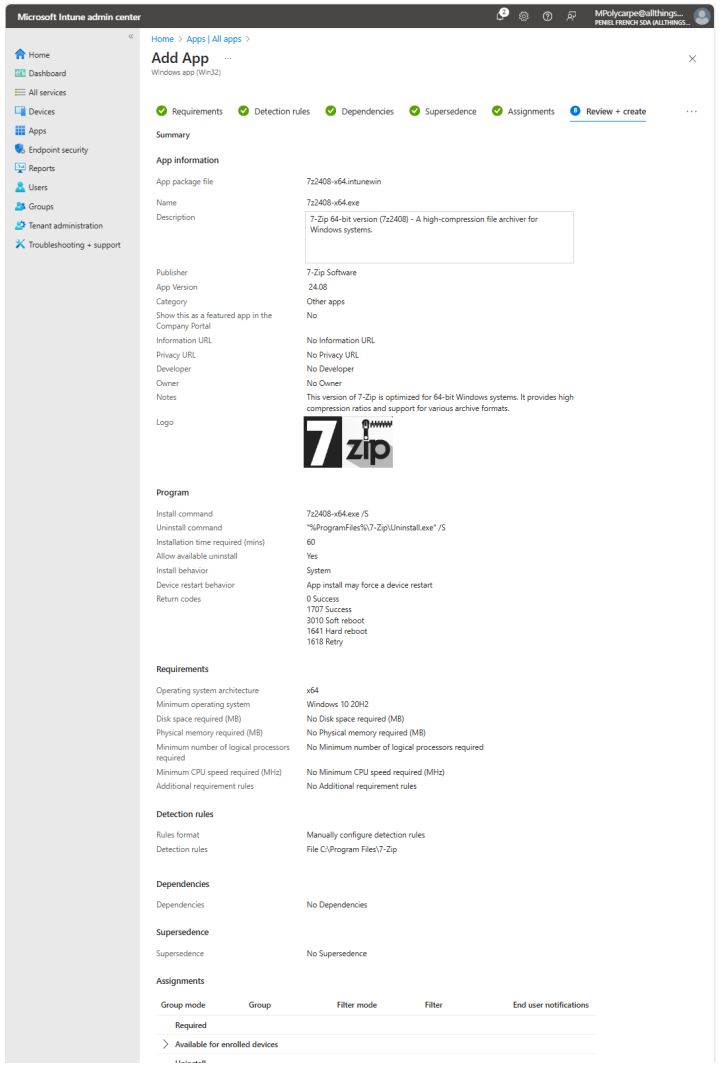
•Gather the Necessary Media:
•Collect the source installer file (e.g., .msi, .exe), along with any required dependencies or supporting files needed for the application's installation.
•Validate the Install and Uninstall Commands:
•Ensure the application has working commands for installation and uninstallation. These commands will be specified during the Intune packaging process (e.g., silent install switches like /quiet or /silent).
•Create the .intunewin File:
•Use the Microsoft Intune Win32 Content Prep Tool to package the application into a .intunewin format, which is required for deployment in Intune.
•Specify:

- •The source folder containing the application files.
- •The setup file (e.g., ZoomInstallerFull.msi).
- •The output folder where the .intunewin file will be saved.

•Ensure File Size Meets Requirements:
•If the total package size exceeds 30GB, clean up unnecessary files and reduce the size to meet the requirements. Applications larger than 30GB cannot be processed by Intune.
•Finalize and Save the .intunewin Package:
•Once the packaging process is complete, the .intunewin file will be ready for upload to the Microsoft Intune Admin Center.

Process flow to Upload Win32 App to Intune





Catalog of All Deployed Apps

Microsoft Intune admin center

MPolycarpe
PENIEL FRENC

Home > Apps

Apps | All apps

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Search

- Overview
- All apps
- Monitor
- By platform
- Windows
- iOS/iPadOS
- macOS
- Android
- Policy
- App protection policies
- App configuration policies
- iOS app provisioning profiles
- S mode supplemental policies
- Policies for Office apps
- Policy sets
- Quiet time

Add | Refresh | Filter | Export | Columns

Search by name or publisher

Name	Type	Status	Version	Assigned
7z2408-x64.exe	Windows app (Win32)		24.08	Yes
Adobe Photoshop	Microsoft Store app (new)			Yes
Board Papers	Microsoft Store app (new)			Yes
Company Portal	Microsoft Store app (new)			Yes
Microsoft 365 Apps for Wi...	Microsoft 365 Apps (Windo...			Yes
Mozilla Firefox	Microsoft Store app (new)			Yes
Netflix	Microsoft Store app (new)			Yes
Notepad++ v8.6.4	Windows app (Win32)		8.6.4	Yes
RdTip Visio Addin	Microsoft Store app (new)			Yes
Skype	Windows app (Win32)		1.0	Yes
vlc-3.0.21-win64.exe	Windows app (Win32)		3.0.21	Yes
vlc-3.0.21-win64.exe (VLC ...	Windows app (Win32)		3.0.21	No
Zoom Rooms Installer	Windows app (Win32)		6.2.5	Yes
Zoom Workplace (64-bit)	Windows app (Win32)		6.2.49583	Yes

The image depicts the "All Apps" section within the Microsoft Intune Admin Center, showcasing a list of deployed applications along with their types, versions, and deployment statuses. The applications include 7z2408-x64.exe (version 24.08), Notepad++ v8.6.4 (version 8.6.4), Skype (version 1.0), vlc-3.0.21-win64.exe, Zoom Rooms Installer (version 6.2.5), and Zoom Workspace (64-bit) (version 6.2.49583). The apps include a mix of Win32 applications, such as .exe or .msi installers, and Microsoft Store apps, highlighting how Microsoft Intune efficiently manages and distributes software across devices.

Microsoft Intune admin center

MPolycarpe@allthings...
PENIEL FRENCH SDA (ALLTHINGS...

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

All services > Devices | Enrollment >

Windows Autopilot devices

Windows enrollment

Refresh | Export | Columns | Sync | Import | Assign user | Delete | Unblock device

10 items loaded

Search | Add filters

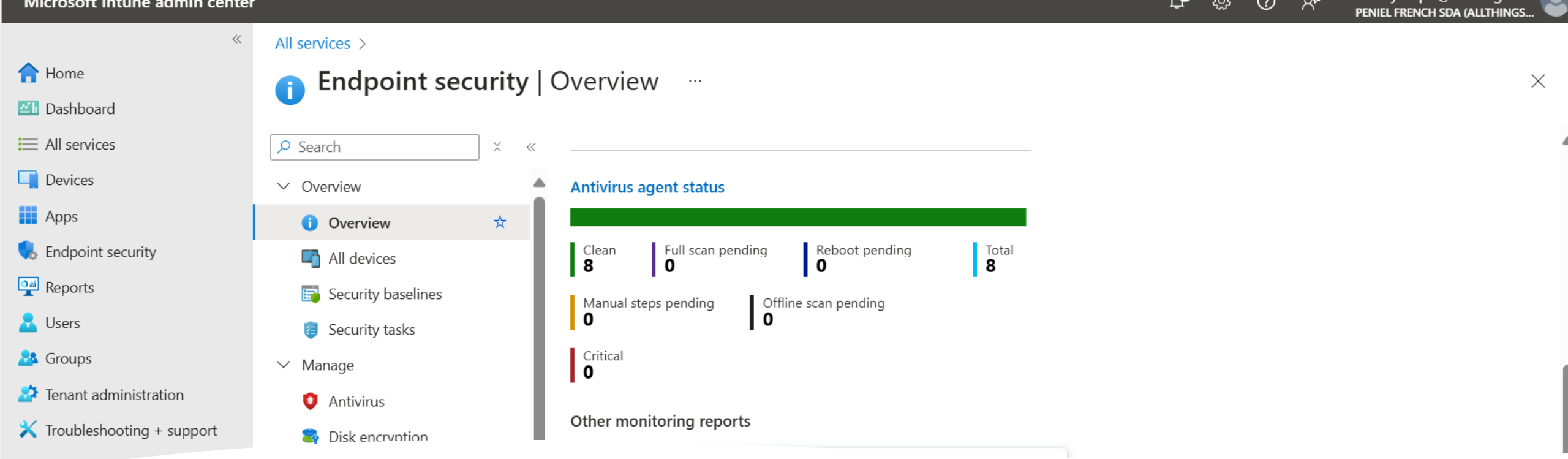
Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.

Last successful sync
12/07/2024, 07:11 PM

Last sync request
12/07/2024, 07:11 PM

Serial number	Manufacturer	Model	Group tag	Profile status	Purchase order	Userless Enrollment Sta...
0010-0266-7144-4202-1607-3278-88	Microsoft Corporation	Virtual Machine		Assigned		Allowed
0836-9116-7101-7997-4016-3718-28	Microsoft Corporation	Virtual Machine		Assigned		Allowed
2665-2266-8837-9800-3537-3517-03	Microsoft Corporation	Virtual Machine		Assigned		Allowed
3136-2590-5660-3803-9571-0915-77	Microsoft Corporation	Virtual Machine		Assigned		Allowed
4294-4234-1578-2791-9581-2763-92	Microsoft Corporation	Virtual Machine		Assigned		Allowed
5321-5858-0120-4292-9461-7966-49	Microsoft Corporation	Virtual Machine		Assigned		Allowed
6318-2632-1070-1023-6583-8428-81	Microsoft Corporation	Virtual Machine		Assigned		Allowed
8296-0716-8824-2639-6446-9462-19	Microsoft Corporation	Virtual Machine		Assigned		Allowed
9073-7827-4861-5126-4743-5795-62	Microsoft Corporation	Virtual Machine		Assigned		Allowed
9922-4930-5768-1209-5428-6685-65	Microsoft Corporation	Virtual Machine		Assigned		Allowed

Enrolled Devices

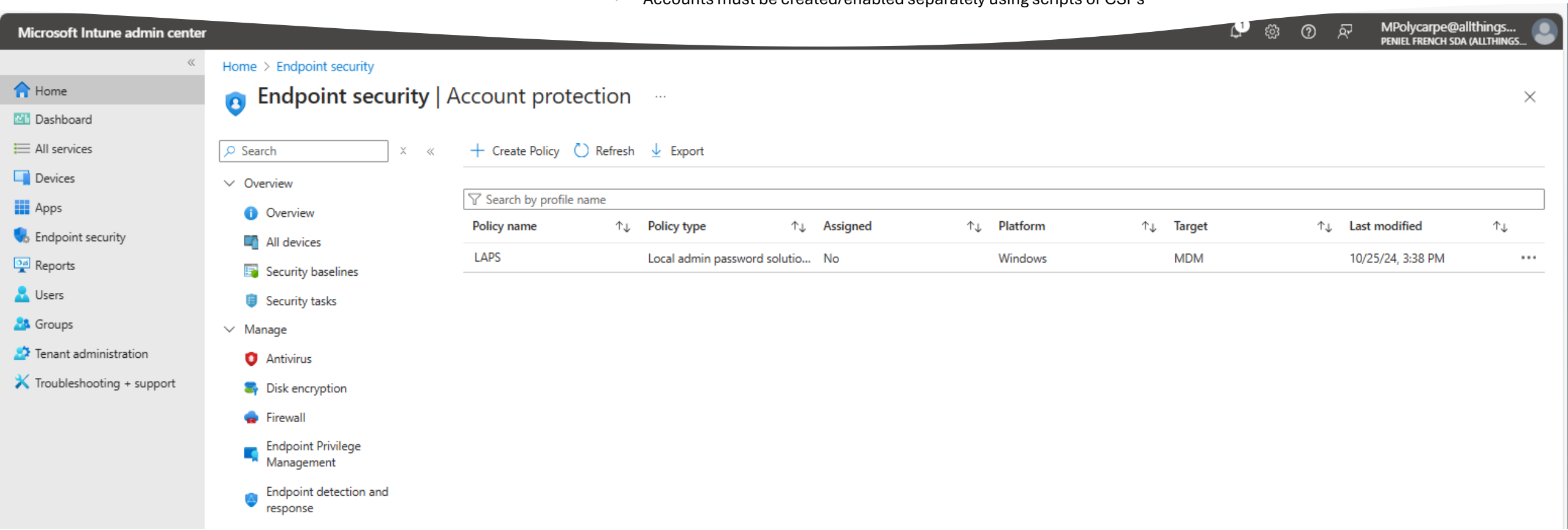


Microsoft Defender Antivirus (MDAV)

- Antivirus Health Overview
  - All metrics for unhealthy endpoints are at zero
  - No devices with active malware
  - Environment is secure
- Policy Details
  - Policy: Microsoft Defender Antivirus
  - Assigned via MDM and Microsoft Sense
  - Latest modification on 10/26/24
- Key Features of MDAV
  - Cloud Protection: Enabled for new threat detection
  - High & Severe Threats: Automatically quarantined
  - Email Scanning: Active to block malicious attachments

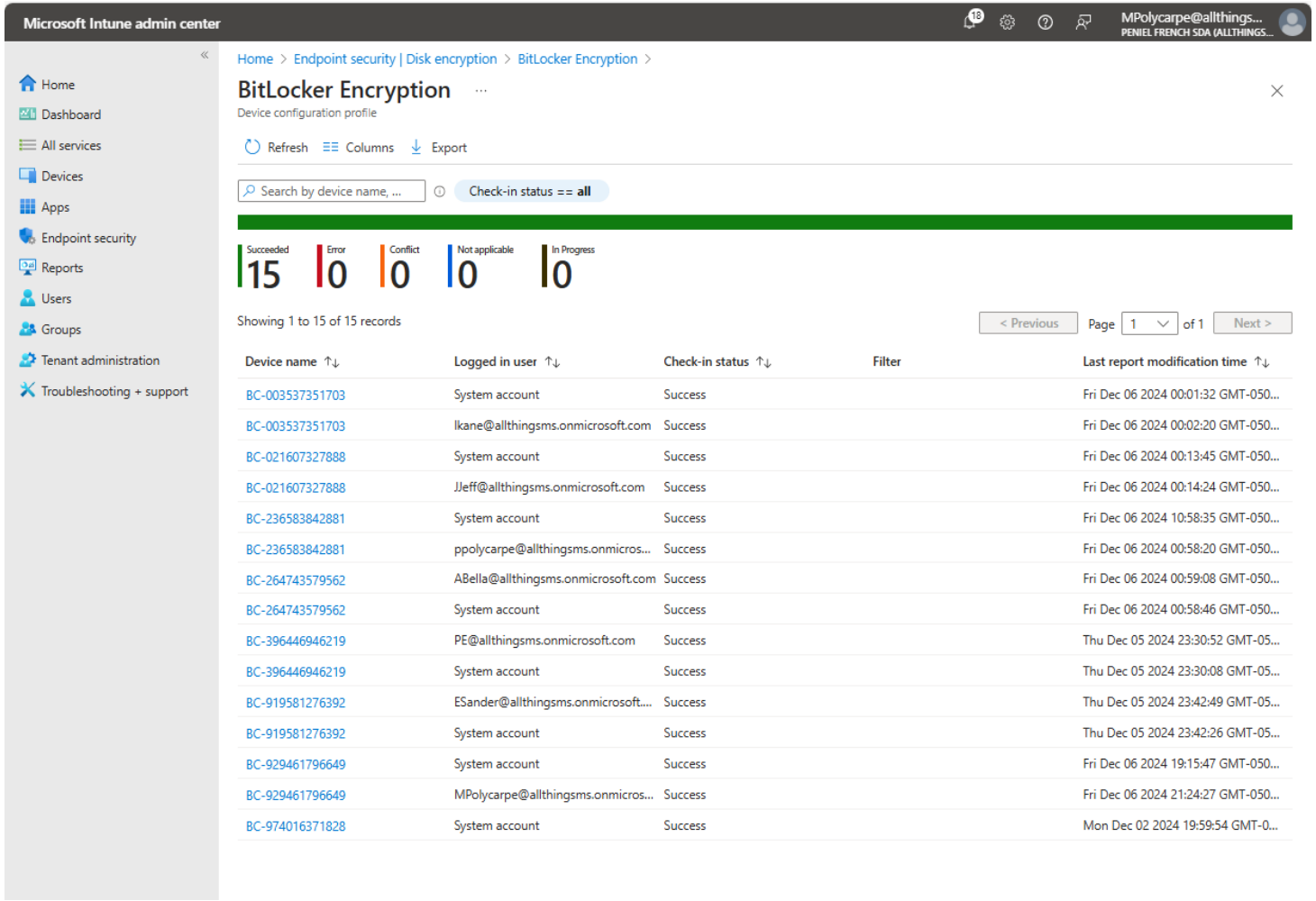
Windows Local Administrator Password Solution (LAPS)

- Purpose of LAPS
  - Securely manage and store passwords for local administrator accounts
- Default Settings
  - Built-in local administrator account is disabled by default
- Use Cases
  - Useful for troubleshooting, support, or device recovery
- Integration with Microsoft Entra
  - Randomizes and stores passwords securely
  - Works with Intune as MDM service
- Account Creation and Enabling
  - LAPS does not create or enable local accounts
  - Accounts must be created/enabled separately using scripts or CSPs



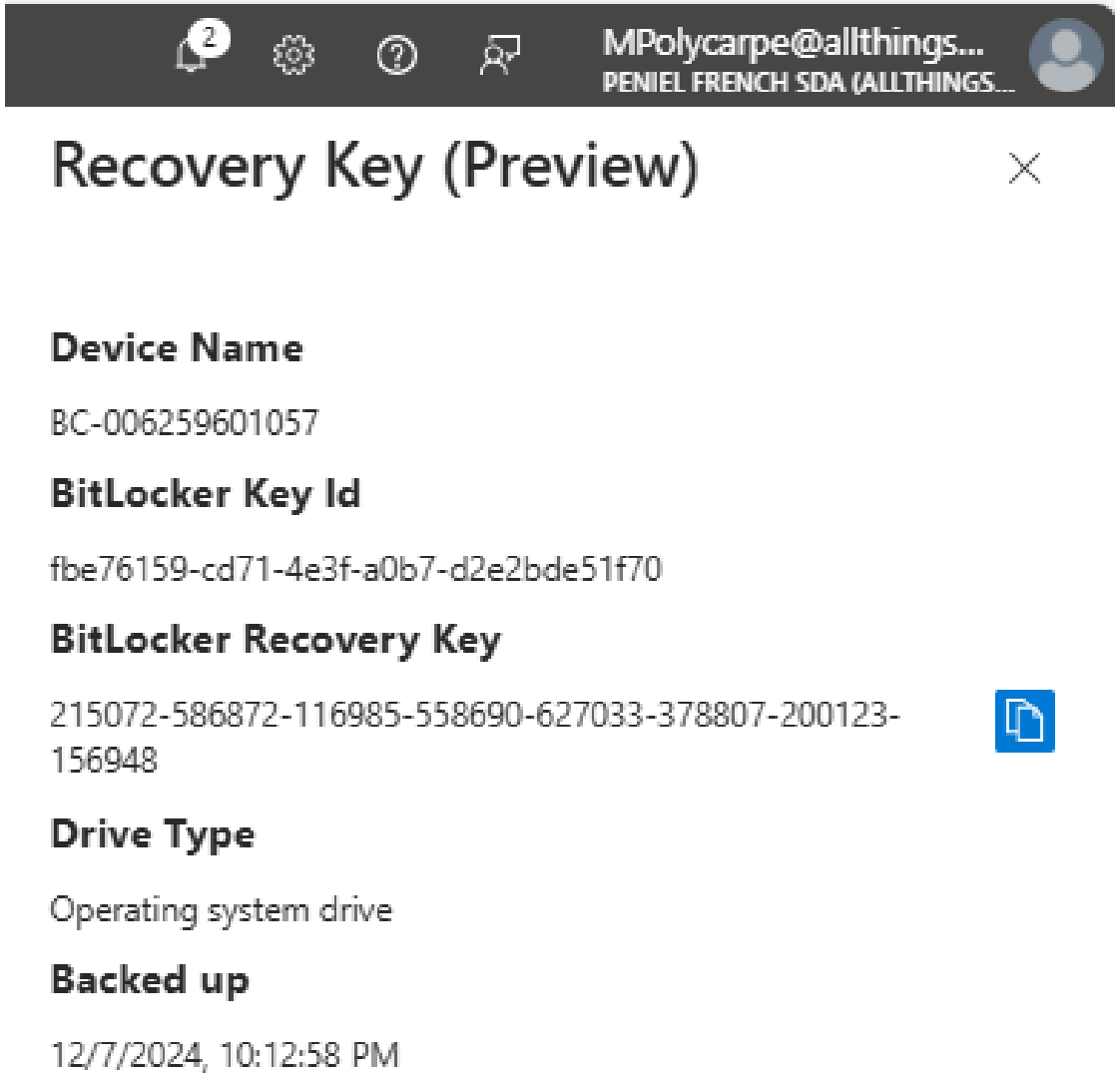
BitLocker Encryption

- BitLocker Encryption Overview
  - Full-disk encryption feature in Windows
  - Secures data by encrypting the entire drive
  - Prevents unauthorized access if a device is lost or stolen
- Policy Configuration in Intune
  - Settings include encryption methods, password rotation, and recovery options
  - Enforces AES-CBC 256-bit for fixed and OS drives
  - Uses AES-CBC 128-bit for removable drives
  - Requires BitLocker recovery keys to be backed up to Active Directory (AD)
- Encryption Types
  - AES-CBC 256-bit: Stronger security, preferred for high-security needs
  - AES-CBC 128-bit: Faster performance, suitable for less critical data

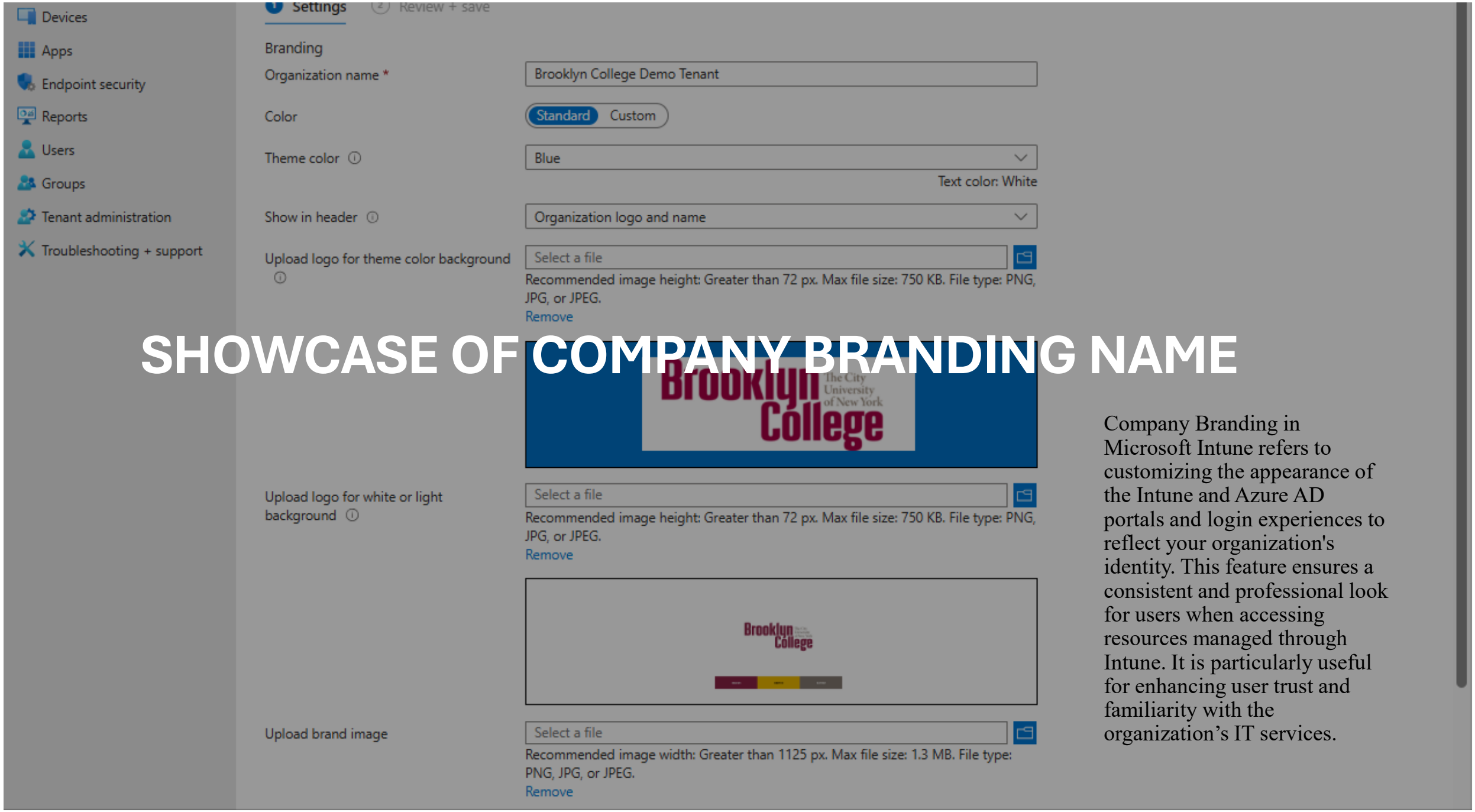


Device name	Logged in user	Check-in status	Filter	Last report modification time
BC-003537351703	System account	Success		Fri Dec 06 2024 00:01:32 GMT-050...
BC-003537351703	lkane@allthingsms.onmicrosoft.com	Success		Fri Dec 06 2024 00:02:20 GMT-050...
BC-021607327888	System account	Success		Fri Dec 06 2024 00:13:45 GMT-050...
BC-021607327888	JJeff@allthingsms.onmicrosoft.com	Success		Fri Dec 06 2024 00:14:24 GMT-050...
BC-236583842881	System account	Success		Fri Dec 06 2024 10:58:35 GMT-050...
BC-236583842881	ppolycarpe@allthingsms.onmicros...	Success		Fri Dec 06 2024 00:58:20 GMT-050...
BC-264743579562	ABella@allthingsms.onmicrosoft.com	Success		Fri Dec 06 2024 00:59:08 GMT-050...
BC-264743579562	System account	Success		Fri Dec 06 2024 00:58:46 GMT-050...
BC-396446946219	PE@allthingsms.onmicrosoft.com	Success		Thu Dec 05 2024 23:30:52 GMT-05...
BC-396446946219	System account	Success		Thu Dec 05 2024 23:30:08 GMT-05...
BC-919581276392	ESander@allthingsms.onmicrosoft....	Success		Thu Dec 05 2024 23:42:49 GMT-05...
BC-919581276392	System account	Success		Thu Dec 05 2024 23:42:26 GMT-05...
BC-929461796649	System account	Success		Fri Dec 06 2024 19:15:47 GMT-050...
BC-929461796649	MPolycarpe@allthingsms.onmicros...	Success		Fri Dec 06 2024 21:24:27 GMT-050...
BC-974016371828	System account	Success		Mon Dec 02 2024 19:59:54 GMT-0...

BitLocker Recovery Keys



SHOWCASE OF COMPANY BRANDING NAME



Company Branding in Microsoft Intune refers to customizing the appearance of the Intune and Azure AD portals and login experiences to reflect your organization's identity. This feature ensures a consistent and professional look for users when accessing resources managed through Intune. It is particularly useful for enhancing user trust and familiarity with the organization’s IT services.

HOURS SPENT LEARNING

SUBSTANTIAL HOURS DEDICATED TO UNDERSTANDING NEW TECHNOLOGIES AND TECHNIQUES

FOCUS ON VIRTUALIZATION AND DEVICE DEPLOYMENT USING WINDOWS AUTOPILOT

- **Documentation and Troubleshooting**
- Extensive reading of Microsoft documentations
- Understanding environmental setup and troubleshooting configurations
- While using the command prompt, there were difficulties in specifying the paths for the source folders. However, after some troubleshooting, the issue was successfully resolved.

- Ran into some issues producing the hash ID to enroll the VMs. After longs hours of troubleshooting, I realize it was related to permission and a minor error in my code.
- Some difficulties arose when performing an Autopilot reset, as one of the devices failed unexpectedly, and I am currently investigating the cause. Additionally, managing BitLocker drive encryption has proven challenging due to various troubleshooting issues.
- Improving the virtual machine's performance, particularly in terms of storage capacity, speed, and efficiency. Access to a device with greater processing power and additional RAM would significantly boost the VM's speed and responsiveness. Furthermore, fine-tuning the VM settings and using SSD storage rather than an HDD could further enhance its overall performance.

Abandoned and Exciting Features

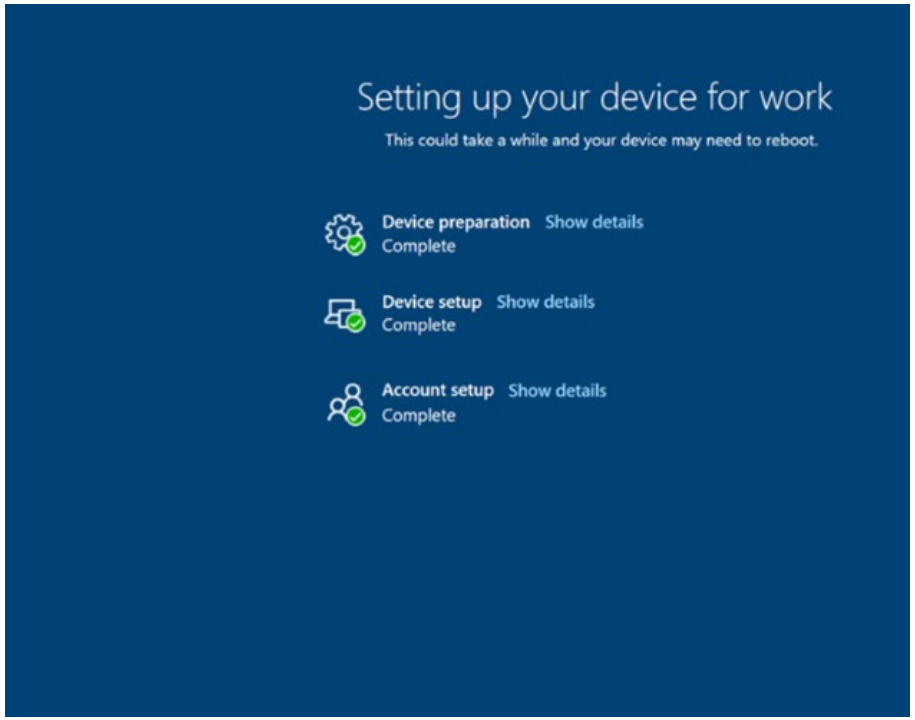
- Technical Challenges Encountered
  - Abandoned rolling out Windows 11 Integration
    - Compatibility issues with Windows 11
  - Technical challenges with Windows Autopilot
  - Errors in virtual machine setup

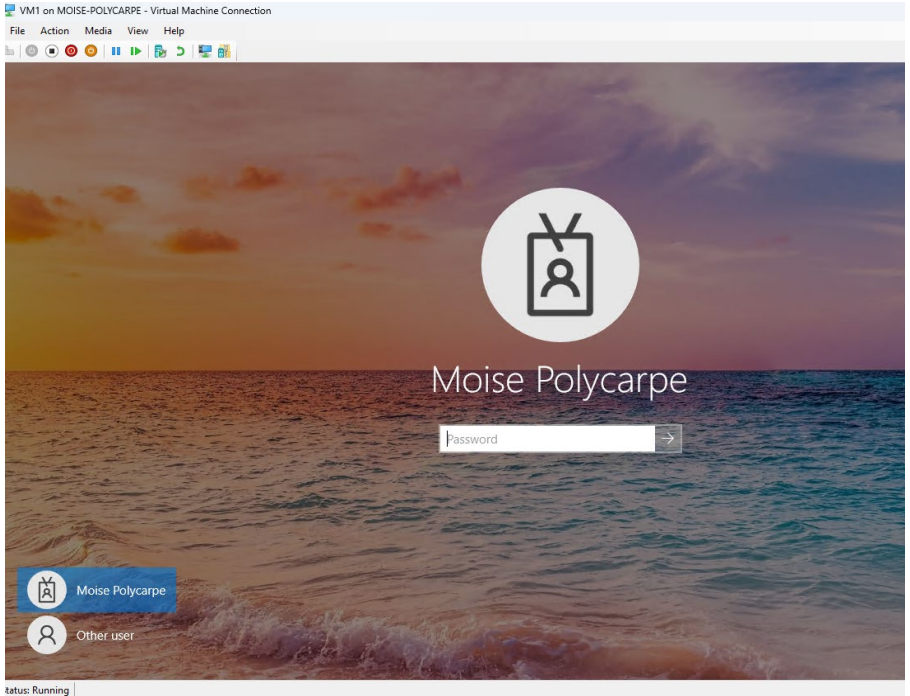
- Exciting Features
  - Configured BitLocker to encrypt all devices
  - Deployed Defender for all endpoints

- These enhancements remind me that as we develop solutions to address real-world challenges, prioritizing security is essential.

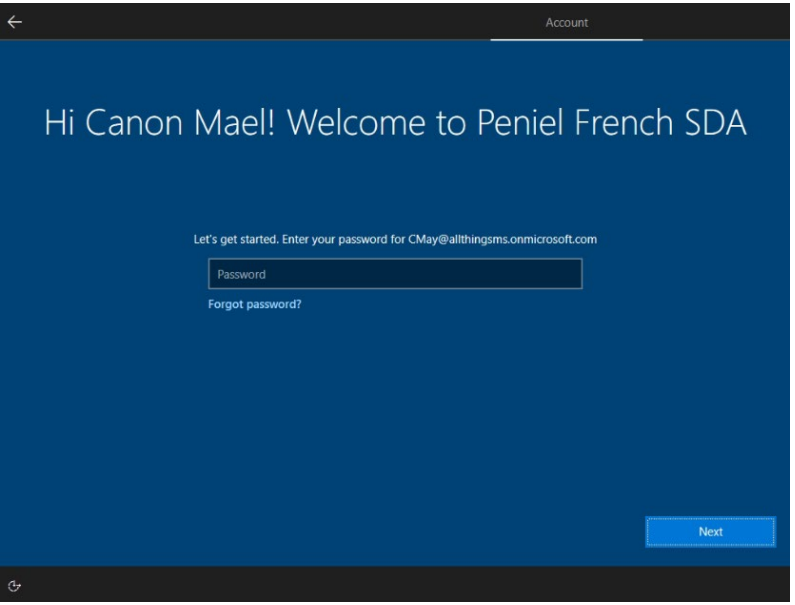
Mockup of the Final Look

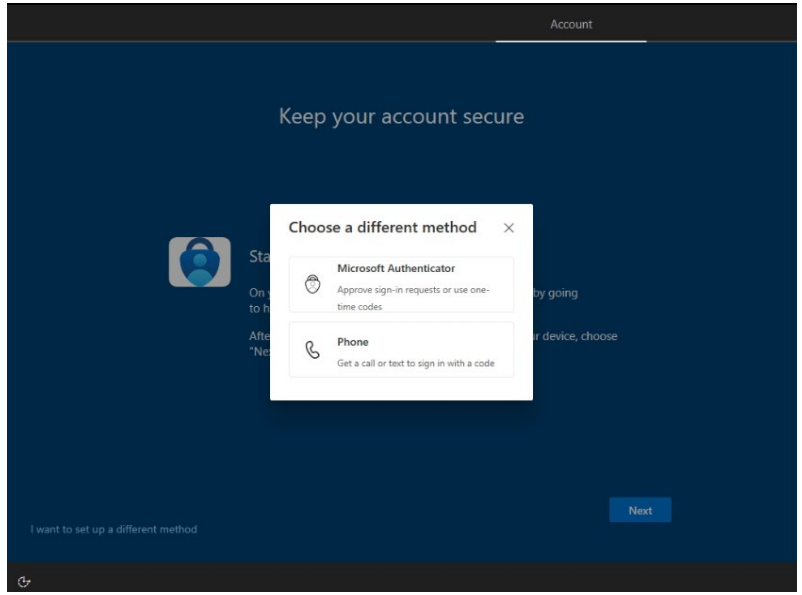
- On the left is a mockup of what a new hire would encounter when accessing company hardware for the first time. Users will need to follow these straightforward steps before they can log in.

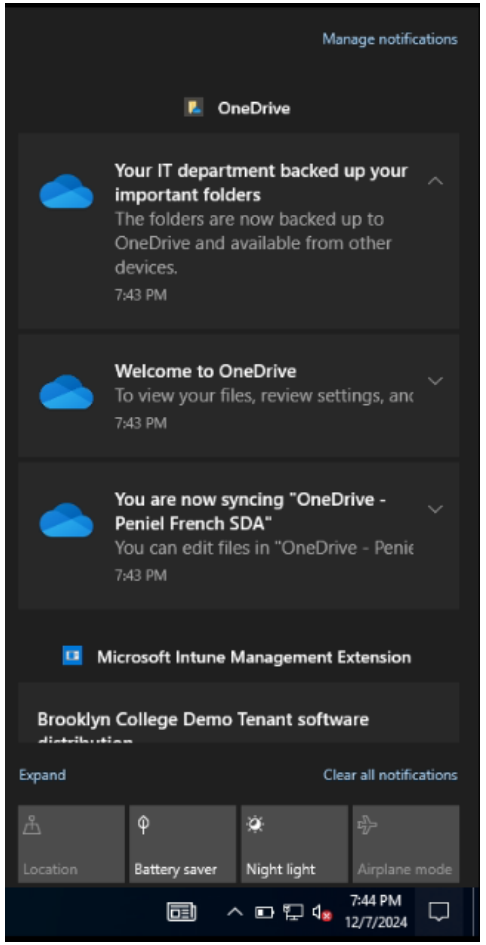




Screen Final Look

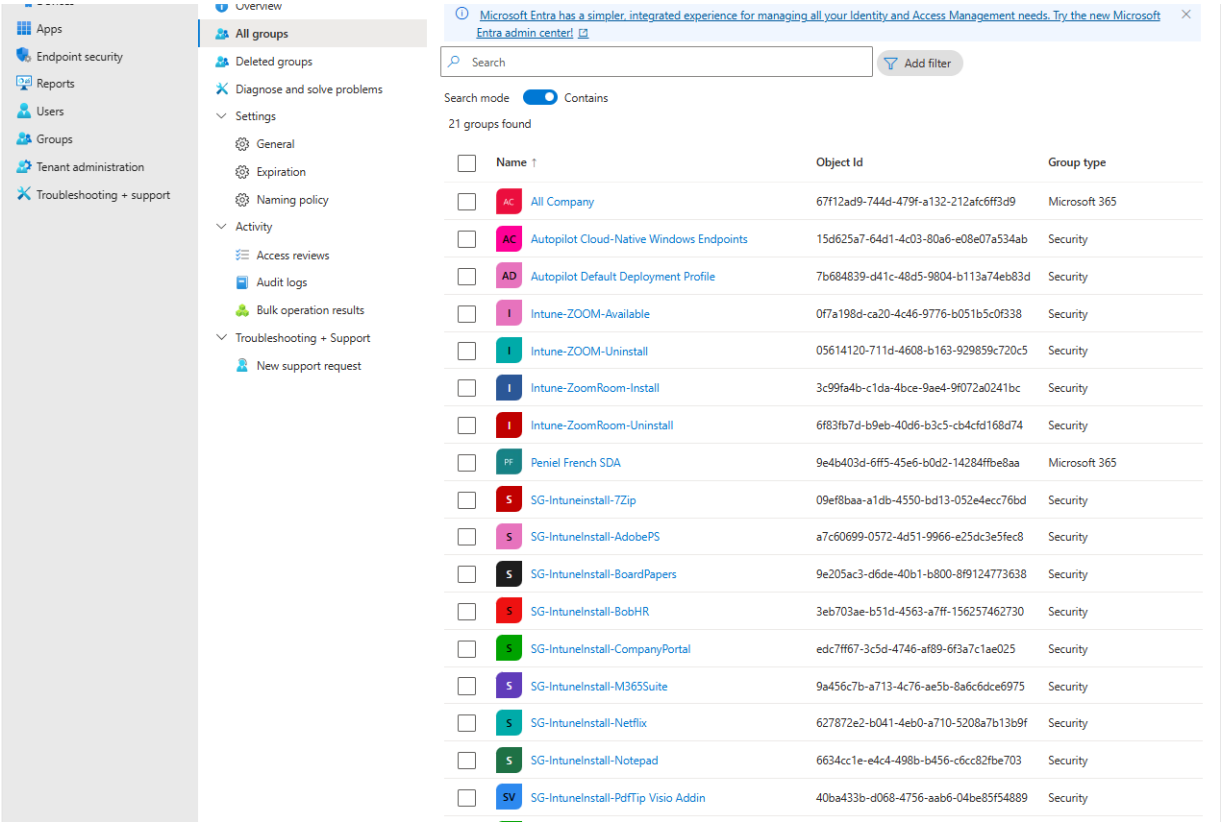






GROUPS OVERVIEW

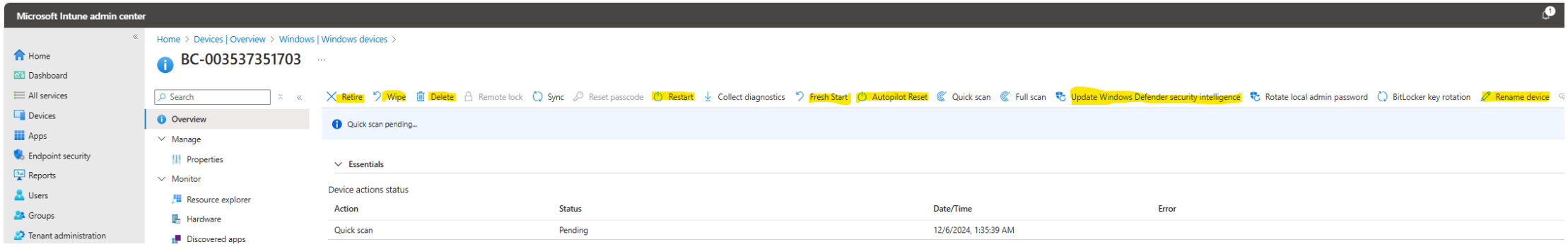
The purpose of security groups in the Microsoft Intune Admin Center for an Autopilot Deployment & Implementation project is to manage and organize users and devices effectively for streamlined deployment, configuration, and policy application. For instance, application deployment: Security groups enable targeted deployment of applications (e.g., Win32 apps like Skype or VLC) to specific users or devices. For example, you can create a group for devices requiring a specific set of productivity tools and deploy the apps exclusively to those devices.



Intune Features

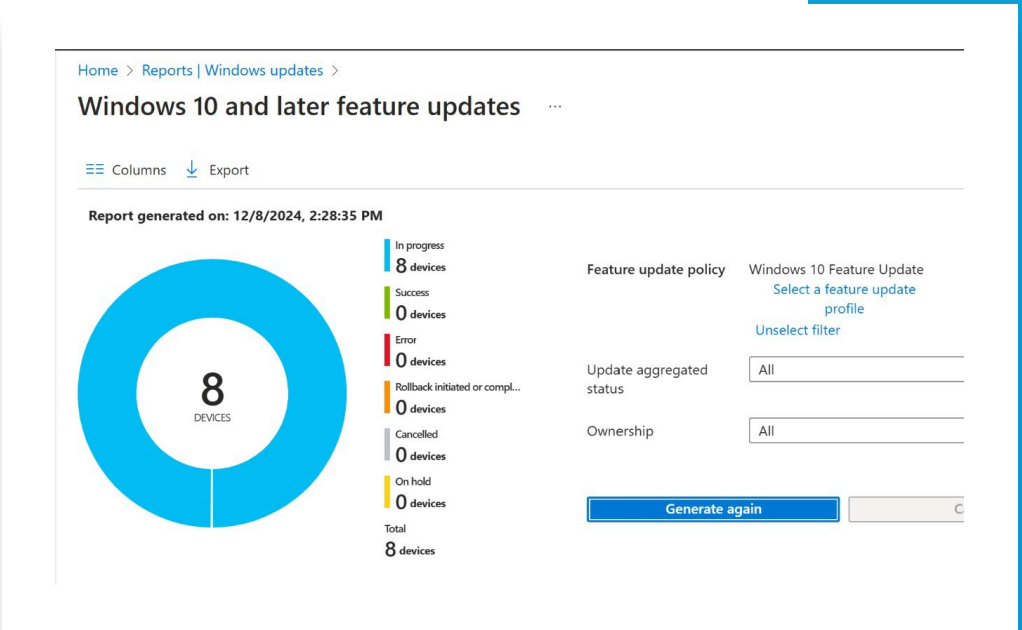
With Intune's features, you can remotely perform various actions. For example:

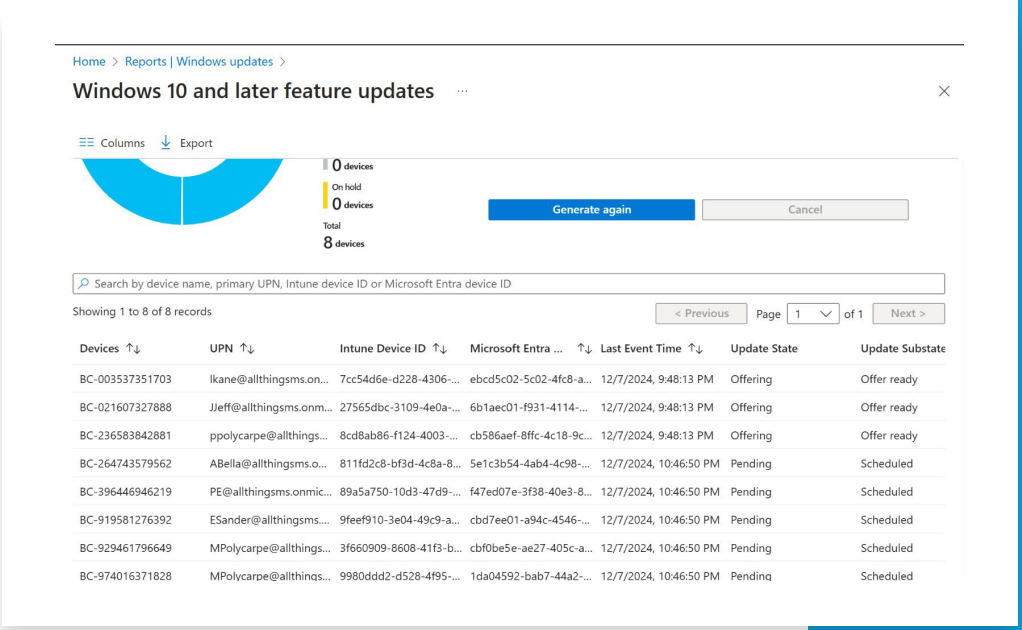
- **Retire**: This option removes a device from Intune management, deleting management policies and configurations while keeping user data intact.
- **Rename Device**: Enables renaming a device directly through the Intune Admin Center.
- **Restart**: Allows you to remotely send a command to restart the device.



Windows Updates

These screenshots collectively provide a detailed overview of the Windows 10 and Later Feature Updates rollout across 8 managed devices. The first screenshot focuses on device-level details and their respective update states, while the second offers a summary view of the overall update progress. All devices are currently in progress, with no errors or completed updates yet.

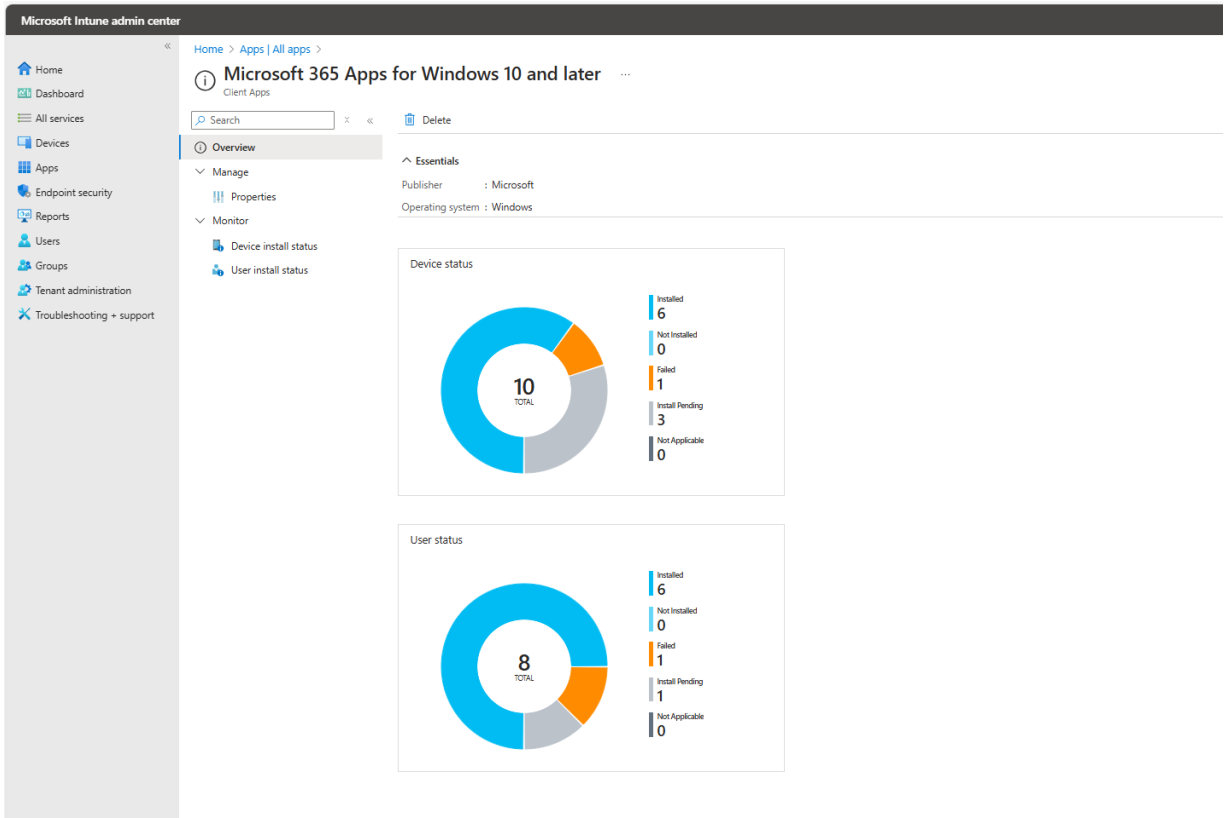


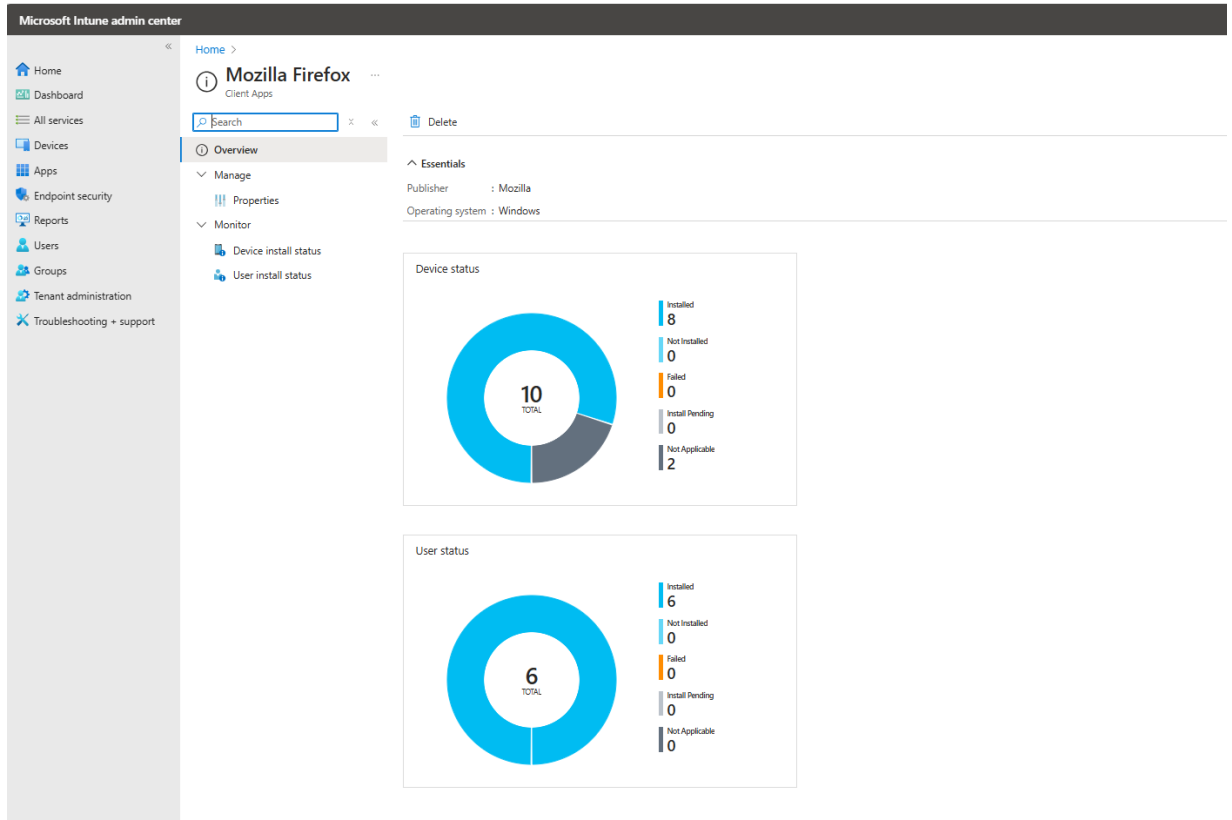


Reports

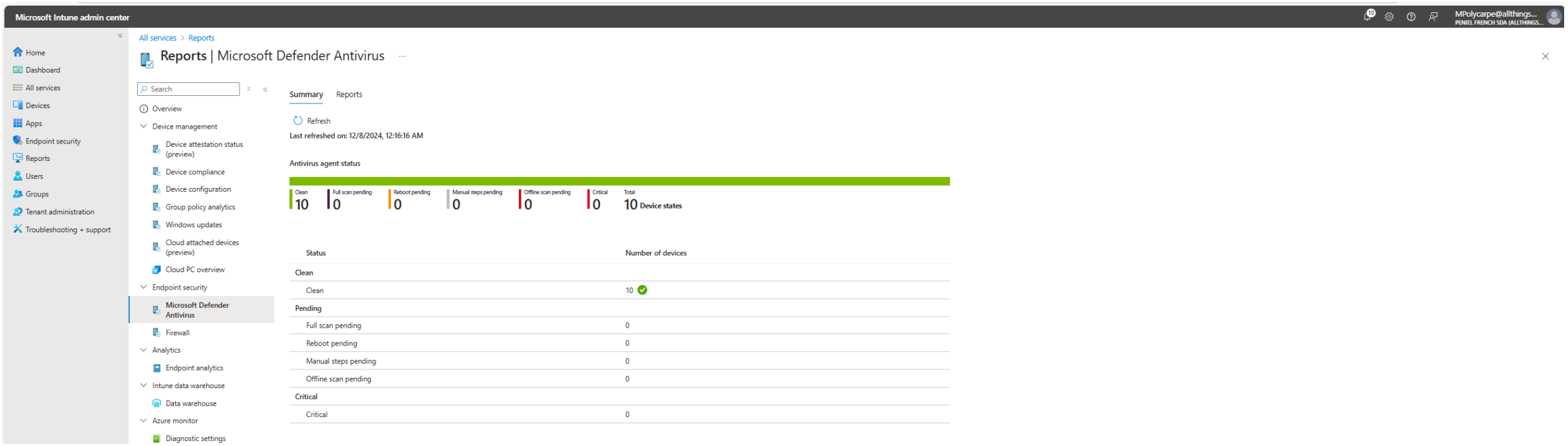

Microsoft Intune admin center
MPolycarpe@allthings...
PENIEL FRENCH SDA (ALLTHINGS...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
All services > Reports
Reports | Device compliance
Search
Overview
Device management
Device attestation status (preview)
Device compliance
Device configuration
Group policy analytics
Windows updates
Cloud attached devices (preview)
Cloud PC overview
Endpoint security
Microsoft Defender Antivirus
Firewall
Analytics
Endpoint analytics
Intune data warehouse
Data warehouse
Azure monitor
Summary
Reports
Refresh
Last refreshed on: 12/8/2024, 12:11:45 AM
Device compliance
Compliant 9 devices
Noncompliant 1 devices
Managed by ConfigMgr 0 devices
Total 10 devices
Device compliance status
Status
Devices
Compliant
Compliant 9
In grace period 0
Noncompliant
Not compliant 0
Not evaluated 1
Other
Managed by Configuration Manager 0

Apps report


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Apps | All apps >
Microsoft 365 Apps for Windows 10 and later
Client Apps
Search
Overview
Manage
Properties
Monitor
Device install status
User install status
Delete
Essentials
Publisher : Microsoft
Operating system : Windows
Device status
10
TOTAL
Installed 6
Not Installed 0
Failed 1
Install Pending 3
Not Applicable 0
User status
8
TOTAL
Installed 6
Not Installed 0
Failed 1
Install Pending 1
Not Applicable 0


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home >
Mozilla Firefox
Client Apps
Search
Overview
Manage
Properties
Monitor
Device install status
User install status
Delete
Essentials
Publisher : Mozilla
Operating system : Windows
Device status
10
TOTAL
Installed 8
Not Installed 0
Failed 0
Install Pending 0
Not Applicable 2
User status
6
TOTAL
Installed 6
Not Installed 0
Failed 0
Install Pending 0
Not Applicable 0

Microsoft Defender Antivirus



Project Summary

The Microsoft Intune Autopilot Deployment & Implementation project was a comprehensive effort to modernize device provisioning and management, involving numerous processes and challenges. It included the detailed Windows Autopilot Deployment Process, covering key requirements, configuration steps, and robust security features to ensure seamless device setup. The project required the creation of dynamic groups and profiles for targeted management, enabling users to join devices to Entra ID, and automating enrollment with Enrollment Status Pages (ESP) for tracking progress. Applications, including Win32 apps, were added and assigned to Intune, following a detailed process flow for packaging, uploading, and deployment. However, numerous challenges arose, particularly with app compatibility, deployment configurations, and device registration, requiring extensive troubleshooting and consuming significant time to resolve.

Security features like BitLocker encryption, Microsoft Defender Antivirus (MDAV), and Windows Local Administrator Password Solution (LAPS) were implemented to enhance protection. The project also included generating device and group reports, showcasing company branding, and providing a catalog of all deployed apps. Despite the challenges, the team resolved issues with systematic troubleshooting, ensuring the successful registration and assignment of devices, the creation of Autopilot profiles, and the monitoring of BitLocker encryption reports. This project reflects a thorough exploration and implementation of Windows Autopilot, demonstrating resilience and dedication to achieving efficient, secure, and scalable device management.

https://github.com/error404progtech/Intune-Autopilot.git

HTTPS://TRELLO.COM/INVITE/B/66EE40796CAD08DA9F66D3BE/ATTI0D4E2E32B3EFDB83D8D9B13E9245336F54DD8877/AUTOPILOT-INTUNE-DEPLOYMENT