

IT 236 Project Report Form

Report Prepared By:	Vivian John Goshashy
Date:	11/26/2025
Project Phase	Mobile Device Management

Section 1: Executive Summary

During this phase of the NewVue Health Infrastructure Modernization Project, cloud-based device management capabilities were introduced through Microsoft Intune. Building on the previously established hybrid identity foundation, NV-CLI was successfully enrolled into Intune and brought under centralized cloud management. This enabled the deployment of Microsoft 365 applications, the application of compliance and security baselines, and the configuration of controlled update management policies.

Verification activities confirmed successful Hybrid Azure AD Join, active Intune enrollment, and the application of cloud-delivered policies and configurations. Collectively, this work demonstrates how modern endpoint management extends from on-premises Active Directory into cloud-native tools, enabling consistent security governance, software deployment, and operational visibility across the organization's Windows devices.

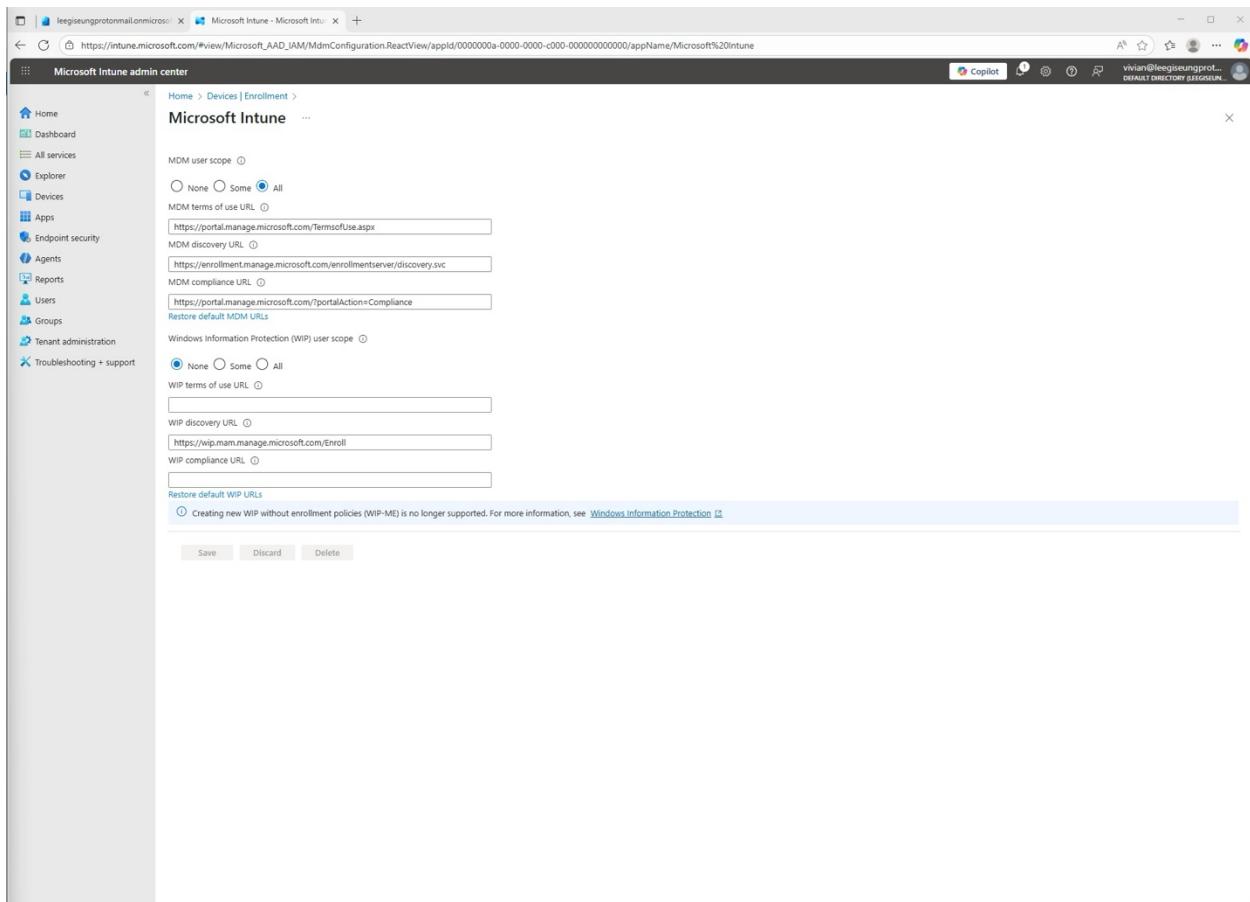
Section 2: Implementation & Verification Evidence

Task 1- Automatic Intune Enrollment Configuration (15 pts)

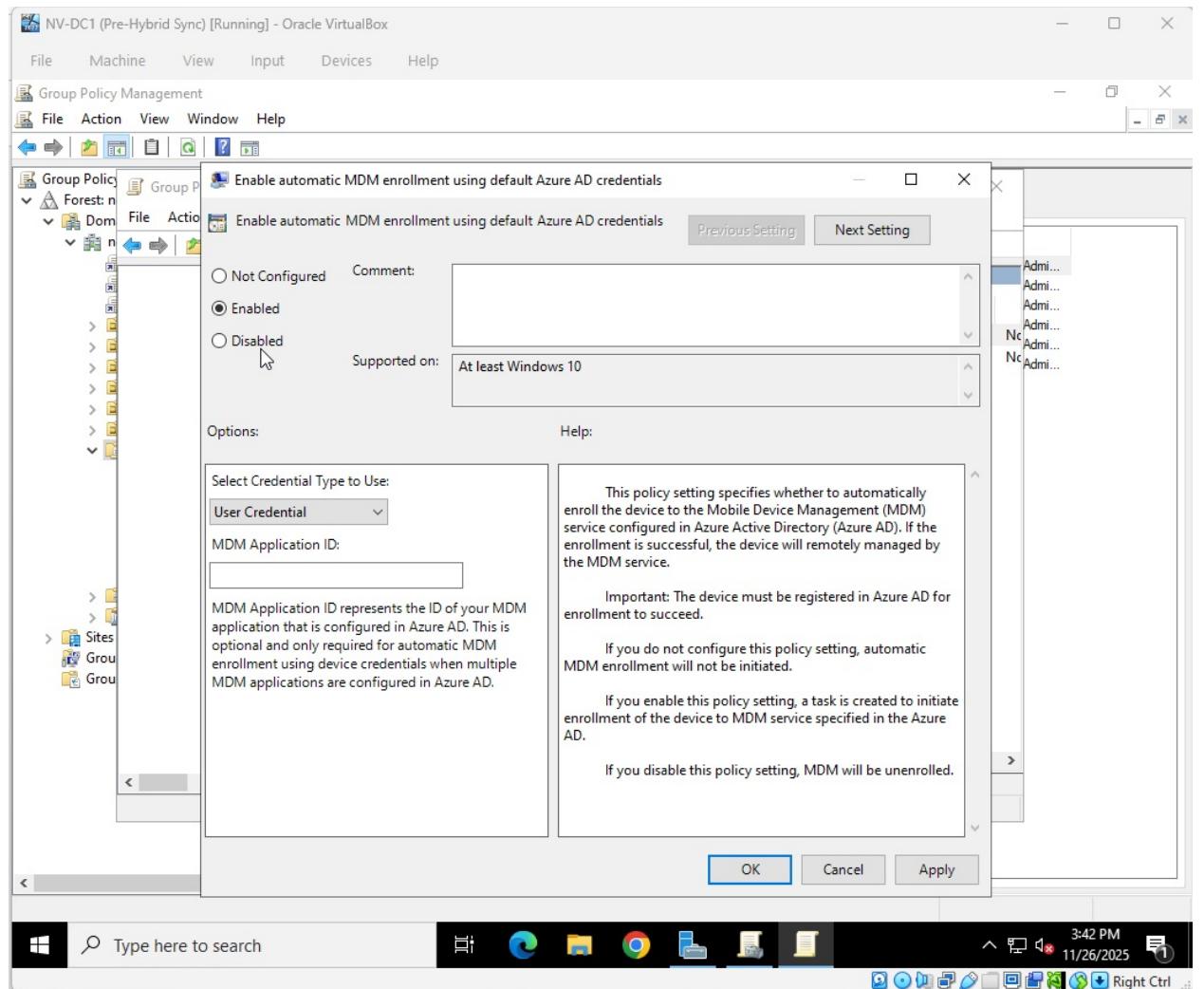
A configuration policy was created to ensure that domain-joined devices are automatically enrolled into Intune during Hybrid Azure AD Join. This step ensures seamless onboarding of corporate Windows endpoints into the organization's cloud management environment.

Required Evidence

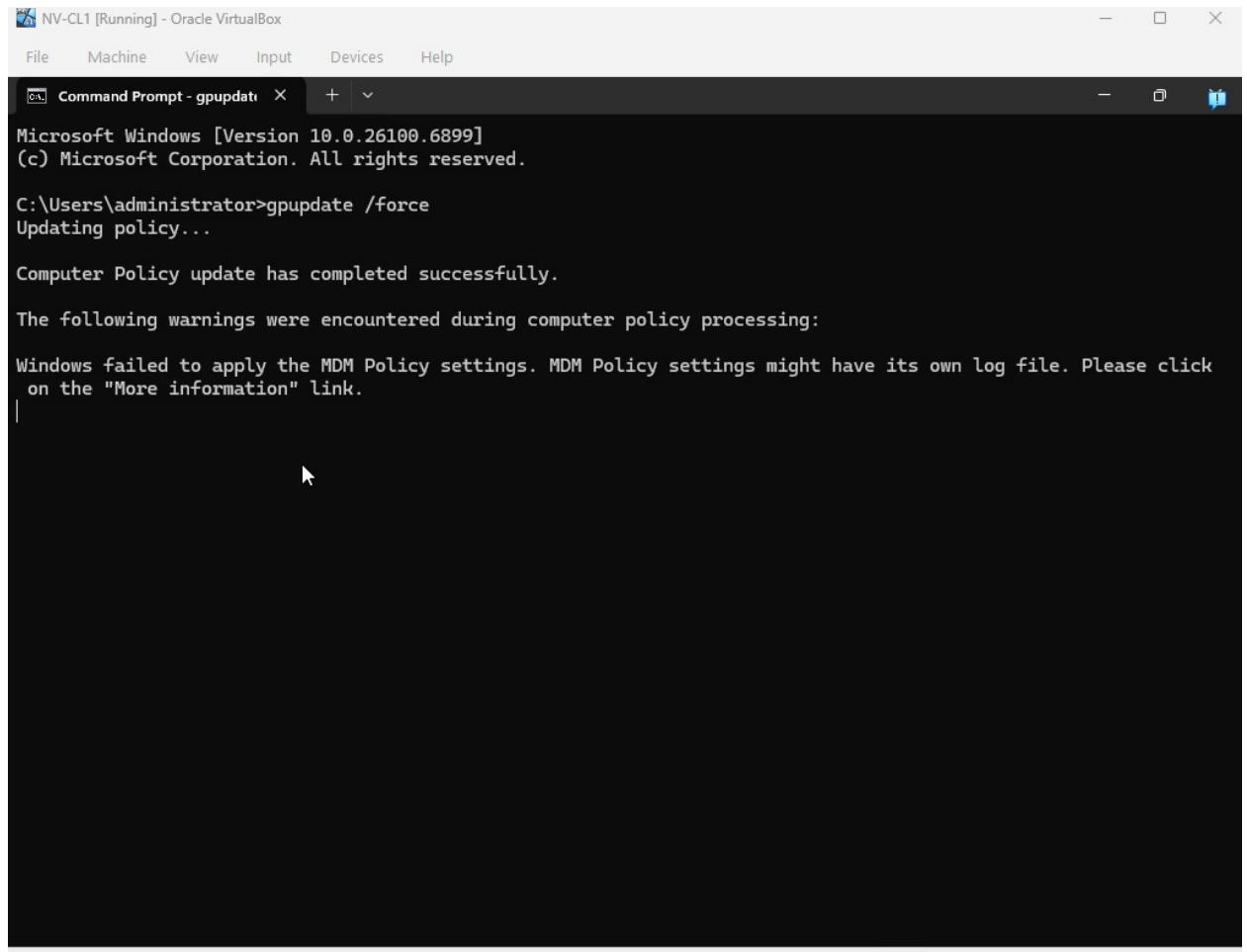
1. Evidence 1: Screenshot showing MDM user scope set to All in Intune.



2. Evidence 2: Screenshot of the GPO “Enable automatic MDM enrollment using default Azure AD credentials” set to **Enabled**.



3. Evidence 3: Screenshot of gpupdate /force executed on NV-CLI.



NV-CL1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Command Prompt - gpupdate X + v

Microsoft Windows [Version 10.0.26100.6899]
(c) Microsoft Corporation. All rights reserved.

C:\Users\administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
The following warnings were encountered during computer policy processing:
Windows failed to apply the MDM Policy settings. MDM Policy settings might have its own log file. Please click on the "More information" link.

5:19 PM 12/1/2025

The screenshot shows a Windows Command Prompt window titled "Command Prompt - gpupdate". The window displays the output of the "gpupdate /force" command. The output indicates that the policy update has completed successfully. It also mentions that Windows failed to apply MDM Policy settings and provides a link for more information. The window is running on a virtual machine named "NV-CL1" in Oracle VirtualBox. The taskbar at the bottom shows various pinned icons and the current date and time (5:19 PM, 12/1/2025).

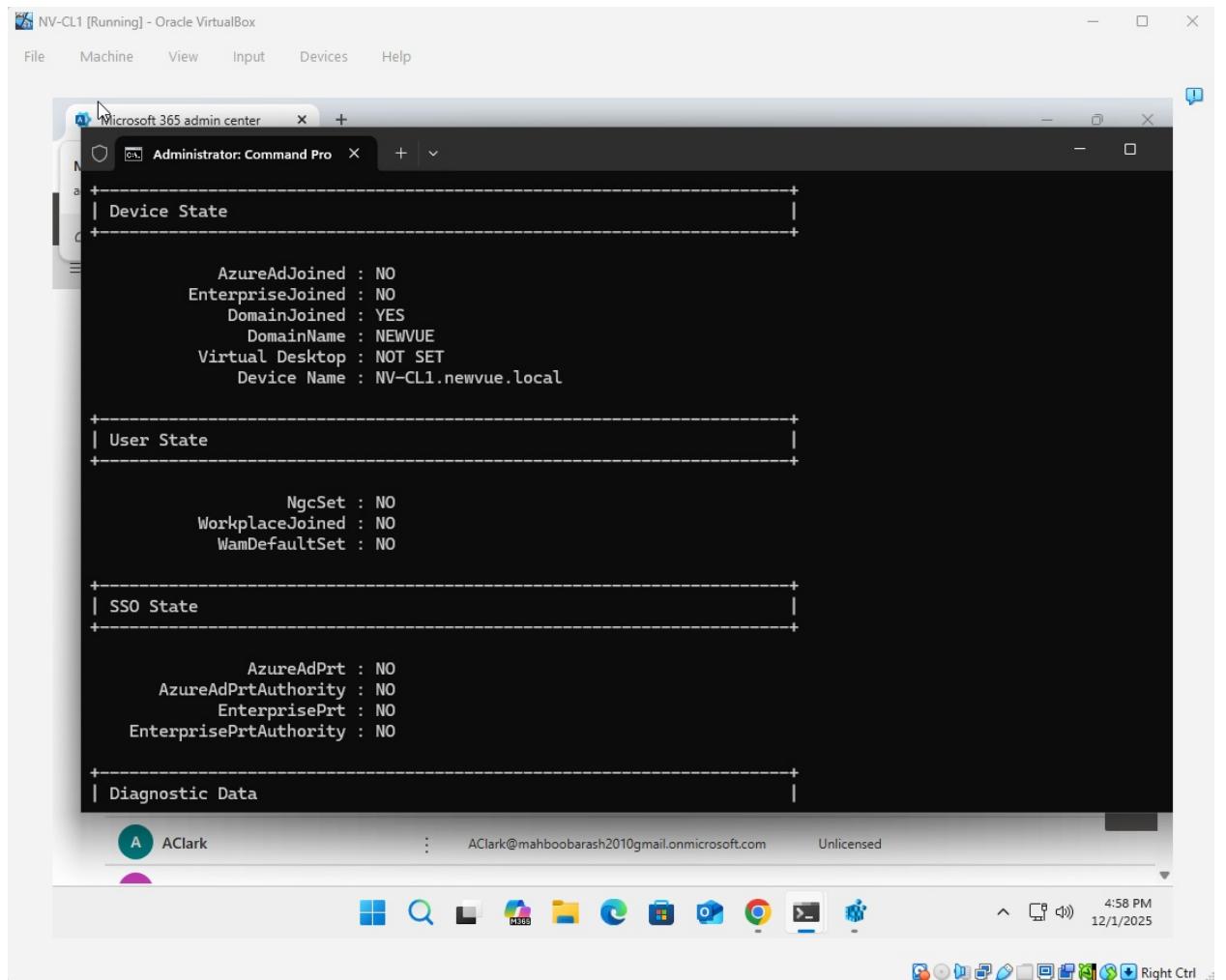
Task 2— Hybrid Azure AD Join & Intune Enrollment Validation

(10 pts)

NV-CLI was validated to confirm successful Hybrid Azure AD Join and Intune MDM enrollment. These verification steps ensure the device is correctly registered and managed through cloud policies.

Required Evidence

4. Evidence 4: Screenshot of dsregcmd /status showing **AzureAdJoined: YES**.



The screenshot shows a terminal window titled "Administrator: Command Pro" running on a Windows operating system. The window displays the output of the command "dsregcmd /status". The output is organized into sections: Device State, User State, SSO State, and Diagnostic Data. In the Device State section, the "AzureAdJoined" value is listed as "YES". The User State section shows "WorkplaceJoined" as "NO". The SSO State section shows "EnterprisePrtAuthority" as "NO". The Diagnostic Data section shows "EnterprisePrtAuthority" as "NO" again. The terminal window also shows the user's profile information at the bottom: AClark, AClark@mahboobash2010gmail.onmicrosoft.com, Unlicensed, and the date/time 12/1/2025 4:58 PM.

```
+-----+  
| Device State |  
+-----+  
        AzureAdJoined : YES  
        EnterpriseJoined : NO  
        DomainJoined : YES  
        DomainName : NEWVUE  
        Virtual Desktop : NOT_SET  
        Device Name : NV-CL1.newvue.local  
+-----+  
| User State |  
+-----+  
        NgcSet : NO  
        WorkplaceJoined : NO  
        WamDefaultSet : NO  
+-----+  
| SSO State |  
+-----+  
        AzureAdPrt : NO  
        AzureAdPrtAuthority : NO  
        EnterprisePrt : NO  
        EnterprisePrtAuthority : NO  
+-----+  
| Diagnostic Data |  
+-----+  
AClark : AClark@mahboobash2010gmail.onmicrosoft.com Unlicensed  
12/1/2025 4:58 PM Right Ctrl
```

5. Evidence 5: Screenshot of NV-CLI listed under Devices → All devices in Intune.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar navigation includes Home, Entra agents, Favorites (Overview, Users, Groups), Devices (Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Account recovery (Preview), Password reset, Custom security attributes, Certificate authorities, External identities, Cross-tenant synchronization, Entra Connect, Domain names, Custom branding, Mobility, Monitoring & health). The main content area is titled 'Devices | All devices' and shows a table with one device entry:

Name	Enabled	OS	Version	Join type	Owner	MDM	Security settings m...	Compliant	Registered %
NV-CLI	Yes	Windows	10.0.26100.6584	Microsoft Entra reg...	Vivian Goshashy	Microsoft Intune	Microsoft Intune	Yes	11/26/2025, 4:40

Below the table, there are sections for Manage (Device settings, Enterprise State Roaming, BitLocker keys, Local administrator password recovery), Activity (Audit logs, Bulk operation results (Preview)), and Troubleshooting + Support (New support request, Diagnose and solve problems).

Task 3— Microsoft 365 (Office) Deployment (10 points)

Microsoft 365 Apps were deployed to NV-CLI using Intune application management. This demonstrated cloud-based application delivery and modern software deployment workflows.

Required Evidence

6. Evidence 6: Screenshot of the Microsoft 365 Apps deployment configuration.

The screenshot shows the Microsoft Intune Admin Center interface for adding a Microsoft 365 App. The left sidebar includes Home, Dashboard, All services (Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, Troubleshooting + support), and a Copilot button. The main content area is titled 'Add Microsoft 365 Apps' under 'App suite information'. It shows the following details:

Name	Microsoft 365 Apps for Windows 10 and later
Description	Microsoft 365 Apps for Windows 10 and later
Publisher	Microsoft
Category	Productivity
Show this as a featured app	No
Information URL	https://products.office.com/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	No Notes
Logo	

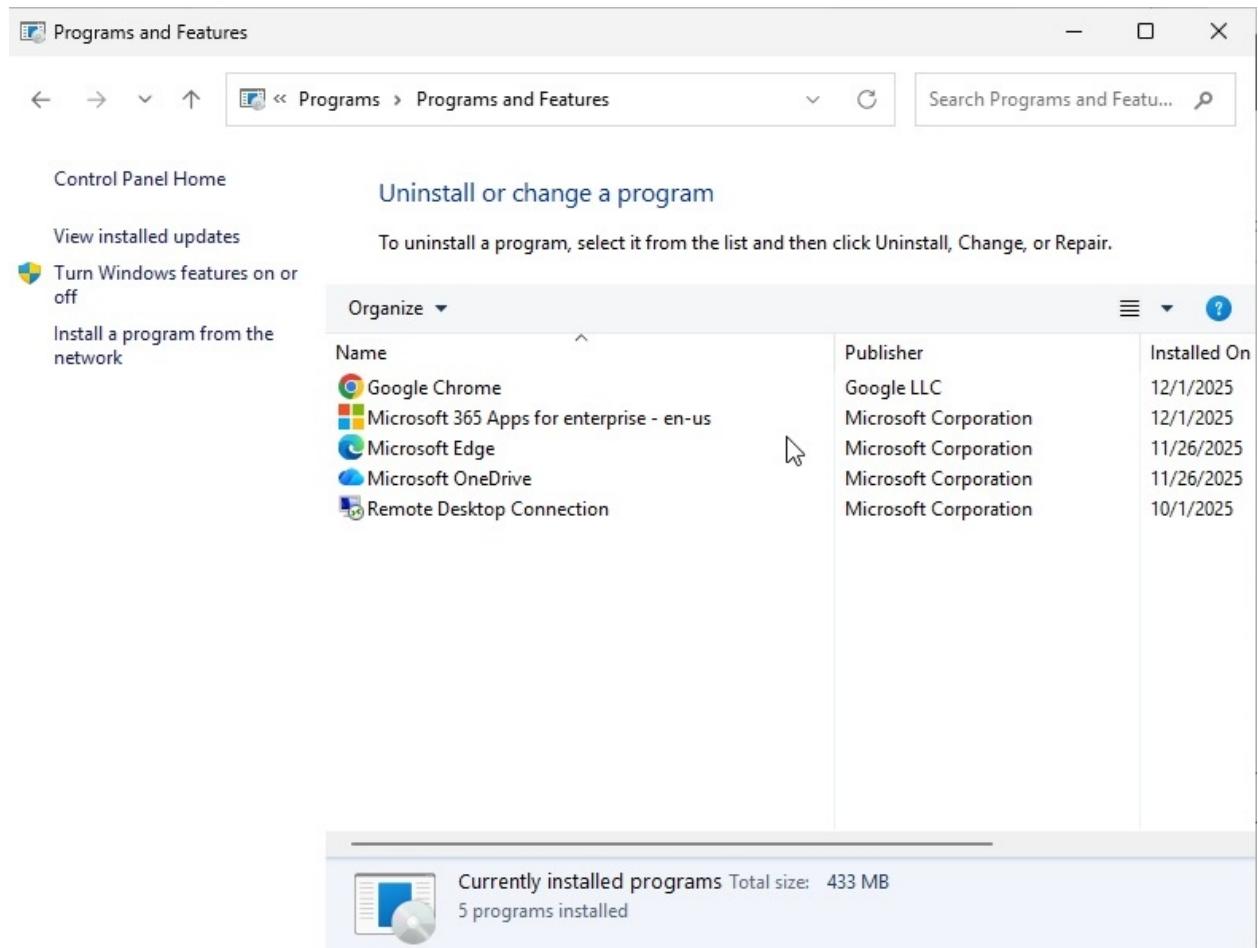
Below this is the 'Configure app suite' section, which lists various settings for the app suite:

Setting	Value
Apps to be installed as part of the suite	Access, Excel, OneNote, Outlook, PowerPoint, Publisher, Teams, Word
Architecture	64-bit
Update channel	Current Channel
Remove other version	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License Terms on behalf of users	Yes
Install background service for Microsoft Search in Bing	Yes
Apps to be installed as part of the suite	1 language(s) selected
Default file format	Office Open Document Format

The 'Assignments' section shows a table with columns: Group mode, Group, Status, Filter mode, and Filter. It contains one row labeled 'Required' with status 'Available for enrolled devices' and a 'Uninstall' link.

At the bottom are 'Previous' and 'Create' buttons.

7. Evidence 7: Screenshot of Office applications appearing on NV-CLI.



Task 4 - Compliance Policies & Security Baseline (20 pts)

A compliance policy and Microsoft Security Baseline were applied to NV-CLI to enforce organizational security requirements.

These policies demonstrate how cloud-managed devices are governed by centralized controls.

Required Evidence

8. Evidence 8: Screenshot of the Compliance Policy assignment.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Windows 10/11 compliance policy" and "Windows 10 and later". It displays tabs for Basics, Compliance settings, Actions for noncompliance, Assignments (which is selected), and Review + create. Under "Included groups", there is a table with one row: "All users" (Status: Active, Group Members: None, Filter mode: None). Under "Excluded groups", there is a note: "When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups." Below this, there is a section for "Add groups" and another table for "Groups" which shows "No groups selected".

9. Evidence 9: Screenshot of NV-CLI compliance status.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "NV-CLI | Device compliance" and shows the "Overview" tab. On the left, a navigation pane under "Manage" has "Device compliance" selected. The main table lists two items:

Policy name	Logged in user	State	User email	Last contacted
Compliance policies	arash@mahboobash2010@gmail.onmicrosoft.com	Compliant		12/01/2025, 04:41
Default Device Compliance Policy	arash@mahboobash2010@gmail.onmicrosoft.com	Compliant		12/01/2025, 04:41

10. Evidence 10: Screenshot of NV-CLI Security Baseline status in Intune.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar navigation includes Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area displays the device details for 'NV-CLI'. The 'Overview' tab is selected. The 'Essentials' section provides the following information:

Device name	:	NV-CL1	Primary user	:	Arash mahboob
Management name	:	arash_Windows_12/1/2025_11:50 PM	Enrolled by	:	Arash mahboob
Ownership	:	Personal	Compliance	:	Compliant
Serial number	:	VirtualBox-68461012-57ea-45bc-84ad-3d93644e7b1e	Operating system	:	Windows
Phone number	:	---	Device model	:	VirtualBox
Device manufacturer	:	innotek GmbH	Last check-in time	:	12/1/2025, 4:47:10 PM
			Remote assistance	:	Not configured

The 'Device actions status' section shows a table with columns Action, Status, Date/time, and Error, indicating 'No data'.

11. Evidence 11: Screenshot of relevant registry paths showing applied baseline settings.

The screenshot shows the Windows Registry Editor window. The left pane displays the registry tree under 'Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\Browser'. The right pane lists the registry keys with their names, types, and data values.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowPasswordManager	REG_DWORD	0x00000000 (0)
AllowPasswordManager_ProviderSet	REG_DWORD	0x00000001 (1)
AllowPasswordManager_WinningProvider	REG_SZ	56C254B6-BE47-4B7C-A84B-33FCCC26104E
AllowSmartScreen	REG_DWORD	0x00000001 (1)
AllowSmartScreen_ProviderSet	REG_DWORD	0x00000001 (1)
AllowSmartScreen_WinningProvider	REG_SZ	56C254B6-BE47-4B7C-A84B-33FCCC26104E
PreventCertErrorOverrides	REG_DWORD	0x00000001 (1)
PreventCertErrorOverrides_ProviderSet	REG_DWORD	0x00000001 (1)
PreventCertErrorOverrides_WinningProvider	REG_SZ	56C254B6-BE47-4B7C-A84B-33FCCC26104E
PreventSmartScreenPromptOverride	REG_DWORD	0x00000001 (1)
PreventSmartScreenPromptOverride_ProviderSet	REG_DWORD	0x00000001 (1)
PreventSmartScreenPromptOverride_WinningProvider	REG_SZ	56C254B6-BE47-4B7C-A84B-33FCCC26104E
PreventSmartScreenPromptOverrideForFiles	REG_DWORD	0x00000001 (1)
PreventSmartScreenPromptOverrideForFiles_ProviderSet	REG_DWORD	0x00000001 (1)
PreventSmartScreenPromptOverrideForFiles_WinningProvider	REG_SZ	56C254B6-BE47-4B7C-A84B-33FCCC26104E

Task 5 - Windows Update Ring Configuration (5 pts)

A Windows Update Ring was created and assigned to devices to control how feature and quality updates are delivered.

This ensures predictable update behavior across hybrid-managed devices.

Required Evidence

Evidence 12: Screenshot of the Update Ring configuration summary.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security (highlighted in orange), Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Create Update ring for Windows 10 and later" under "Windows 10 and later". It shows three completed steps: Basics, Update ring settings, and Assignments, with a fourth step, "Review + create", currently selected. The "Basics" section shows a Name of "NewVue – Update Ring" and a Description of "No Description". The "Update ring settings" section contains various configuration options, many of which are set to "Allow": Microsoft product updates, Windows drivers, Quality update deferral period (days), Feature update deferral period (days), Upgrade Windows 10 devices to Latest Windows 11 release, Set feature update uninstall period (2 - 60 days), Servicing channel (General Availability channel), User experience settings (Automatic update behavior: Auto install at maintenance time, Active hours start: 8 AM, Active hours end: 5 PM, Option to pause Windows updates: Enable, Option to check for Windows updates: Enable, Change notification update level: Use the default Windows Update notifications, Use deadline settings: Not configured). The "Assignments" section shows "Included groups" with "All devices" and "All users" listed as active. The "Excluded groups" section shows a table with one row: "No results."

Task 6 - Remote Device Actions (10 pts)

Basic remote management actions were executed from the Intune Admin Center, such as Sync or Restart. This demonstrates remote control and cloud-based management capabilities.

Required Evidence

Evidence 13: Screenshot of the available Remote Actions for NV-CLI.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation links: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security (highlighted in orange), Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Create Update ring for Windows 10 and later" under "Windows 10 and later". The "Update ring settings" tab is selected, indicated by a green checkmark. The page includes sections for "Update settings" and "User experience settings". In the "Update settings" section, there are fields for "Microsoft product updates" (Allow/Block), "Windows drivers" (Allow/Block), "Quality update deferral period (days)" (set to 2), "Feature update deferral period (days)" (set to 7), "Upgrade Windows 10 devices to Latest Windows 11 release" (Yes/No, set to No), "Set feature update uninstall period (2 - 60 days)" (set to 10), "Enable pre-release builds" (Enable/Not Configured, set to Not Configured), and "Select pre-release channel" (set to Windows Insider - Release Preview). In the "User experience settings" section, there are fields for "Automatic update behavior" (Auto install at maintenance time), "Active hours start" (8 AM), "Active hours end" (5 PM), "Option to pause Windows updates" (Enable/Disable, set to Enable), "Option to check for Windows updates" (Enable/Disable, set to Enable), "Change notification update level" (Use the default Windows Update notifications), "Use deadline settings" (Allow/Not configured, set to Not configured), "Deadline for feature updates" (Number of days, 0 to 30), "Deadline for quality updates" (Number of days, 0 to 30), "Grace period" (Number of days, 0 to 7), and "Auto reboot before deadline" (Yes/No, set to No).

Evidence 14: Screenshot confirming execution of one action (e.g., Sync completed).

The screenshot shows the Microsoft Endpoint Manager (Intune) interface for managing devices. The left sidebar lists various management categories: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, and Groups. The main area displays details for a device named 'NV-CL1'. The 'Overview' tab is selected. The 'Essentials' section provides basic information about the device, including its name ('NV-CL1'), management name ('arash_Windows_12/1/2025_11:50 PM'), ownership ('Personal'), serial number ('VirtualBox-68461012-57ea-45bc-84ad-3d93644e7b1e'), phone number ('***'), and manufacturer ('innotek GmbH'). To the right of the essentials, there is a list of actions with icons: Update Windows Defender security intelligence (blue gear), BitLocker key rotation (key icon), Rename device (pencil icon), New remote assistance session (phone icon), Locate device (location pin icon), Pause config refresh (down arrow icon), Run remediation (preview) (triangle icon), and Not configured (greyed-out). A search bar and several global navigation buttons (Retire, Wipe, Delete, Remote lock, Sync, Reset passcode, Restart, Fresh Start, Autopilot Reset, Quick scan, Full scan) are also visible at the top.

Task 7 - Device Reporting & Hardware Inventory (10 pts)

Intune reporting features were reviewed to confirm device health, hardware information, and compliance details.

This ensures administrators can accurately track device state and configuration.

Required Evidence

Evidence 15: Screenshot of the Hardware information page for NV-CLI.

The screenshot shows the Microsoft Intune Admin Center interface. The left sidebar contains navigation links such as Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area displays the hardware information for a device named NV-CL1. The navigation bar at the top shows the path: Home > Devices | Overview > Windows | Windows devices > NV-CL1. The title of the page is "NV-CL1 | Hardware". The left sidebar under the "Hardware" section includes options like Discovered apps, Device compliance, Device configuration, App configuration, Recovery keys, User experience, Group membership, Managed Apps, Filter evaluation, Enrollment, and Remediations (preview). The main content area is divided into several sections: System, Operating system, Storage, System enclosure, Network details, and Network service. Key data points include:

System	Value
Name	NV-CL1
Management name	arash_Windows_12/1/2025_11:50 PM
Intune Device ID	424355ca-aab7-4f6e-b760-605f8ec8f214
Microsoft Entra Device ID	424355ca-aab7-4f6e-b760-605f8ec8f214
Serial number	VirtualBox-68461012-57ea-45bc-84ad-3d93644e7b1e
Enrollment profile	

Operating system	Value
Operating system	Windows
Operating system version	10.0.26100.6899
Operating system language	en-US
Operating system edition	Pro
Operating system SKU	Windows 10/11 Professional (48)

Storage	Value
Total storage space	79.17 GB
Free storage space	43.48 GB

System enclosure	Value
IMEI	
MEID	
Manufacturer	innotek GmbH
Model	VirtualBox
Processor Architecture	x64
Phone number	
TPM Version	
TPM manufacturer ID	
TPM manufacturer version	
System management BIOS version	

Network details	Value
Subscriber carrier	
Cellular technology	
Wi-Fi MAC	
Ethernet MAC	080027B78A98
ICCID	
Wi-Fi IPv4 address	
Wi-Fi subnet ID	
Wired IPv4 address	10.0.2.18

Network service	Value
Enrolled date	12/1/2025 3:50:39 PM

Evidence 16: Screenshot of the Device Compliance overview for NV-CLI.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar navigation includes Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "NV-CLI | Device compliance" and displays the "Overview" section. It features a search bar, refresh, export, and column settings buttons. A table lists two items under "Compliance policies": "Compliance policies" (logged in user: arash@mahboobarash2010@gmail.onmicro, state: Compliant) and "Default Device Compliance Policy" (logged in user: arash@mahboobarash2010@gmail.onmicro, state: Compliant). The table also includes columns for User email and Last contacted. On the left, a sidebar under "Manage" shows "Device compliance" selected, with sub-options: Device configuration, App configuration, Recovery keys, User experience, Group membership, Managed Apps, Filter evaluation, Enrollment, and Remediations (preview).

Policy name	Logged in user	State	User email	Last contacted
Compliance policies	arash@mahboobarash2010@gmail.onmicro	Compliant		12/01/2025, 04:41
Default Device Compliance Policy	arash@mahboobarash2010@gmail.onmicro	Compliant		12/01/2025, 04:41