

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.

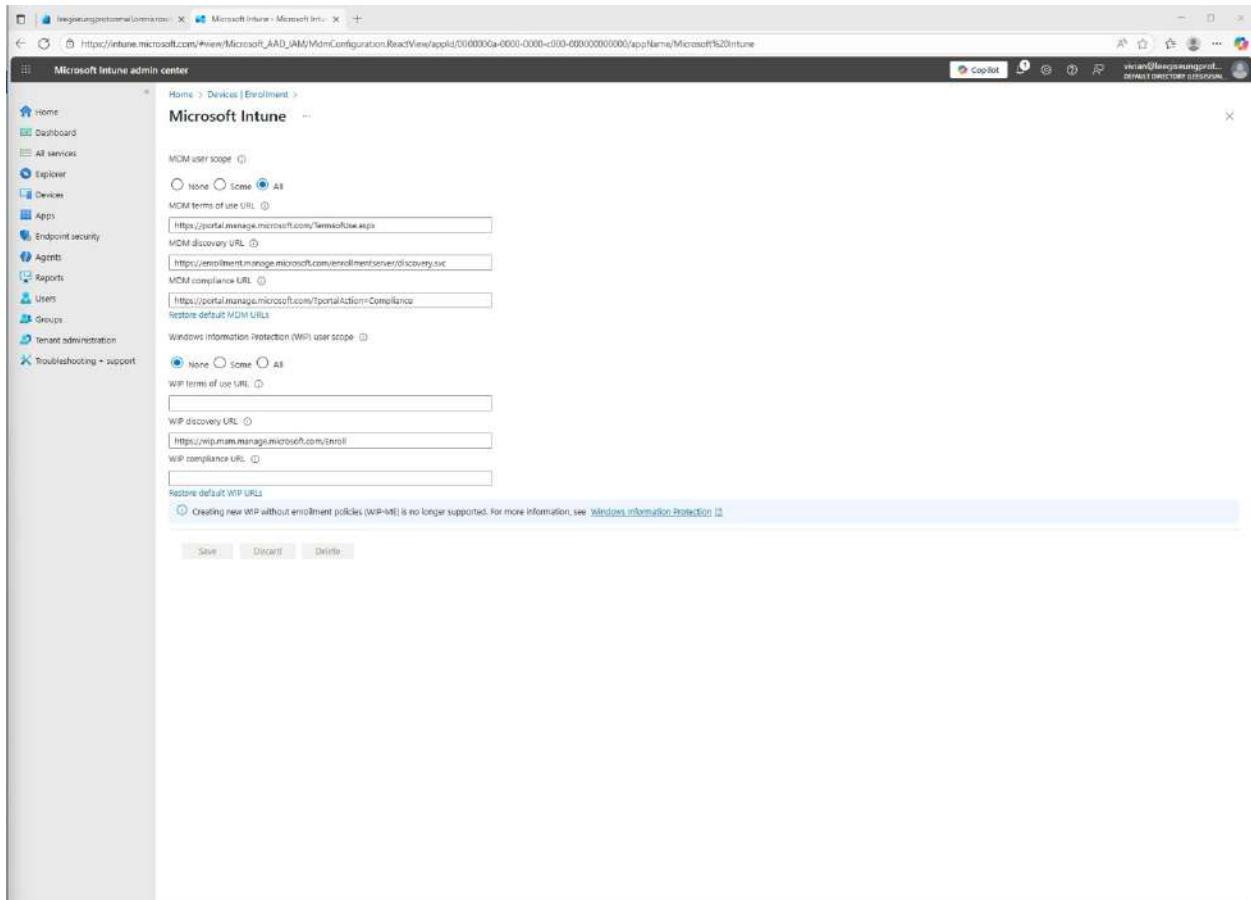
Section 2: Implementation & Verification Evidence

Task 1- Automatic Intune Enrollment Configuration (15 pts)

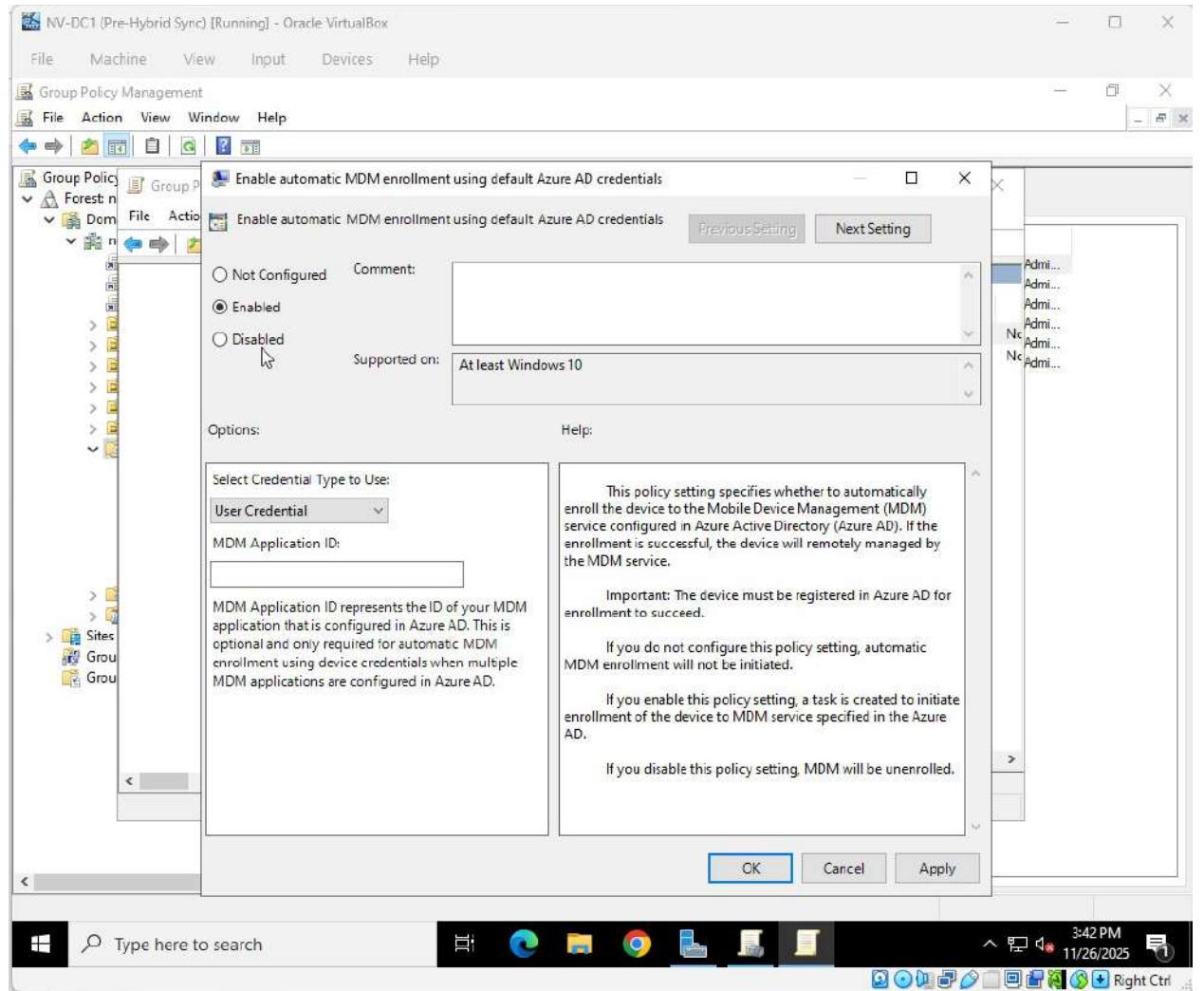
A configuration policy was created to ensure that domain-joined devices are automatically enrolled into Intune during Hybrid Azure AD Join. This step ensures seamless onboarding of corporate Windows endpoints into the organization's cloud management environment.

Required Evidence

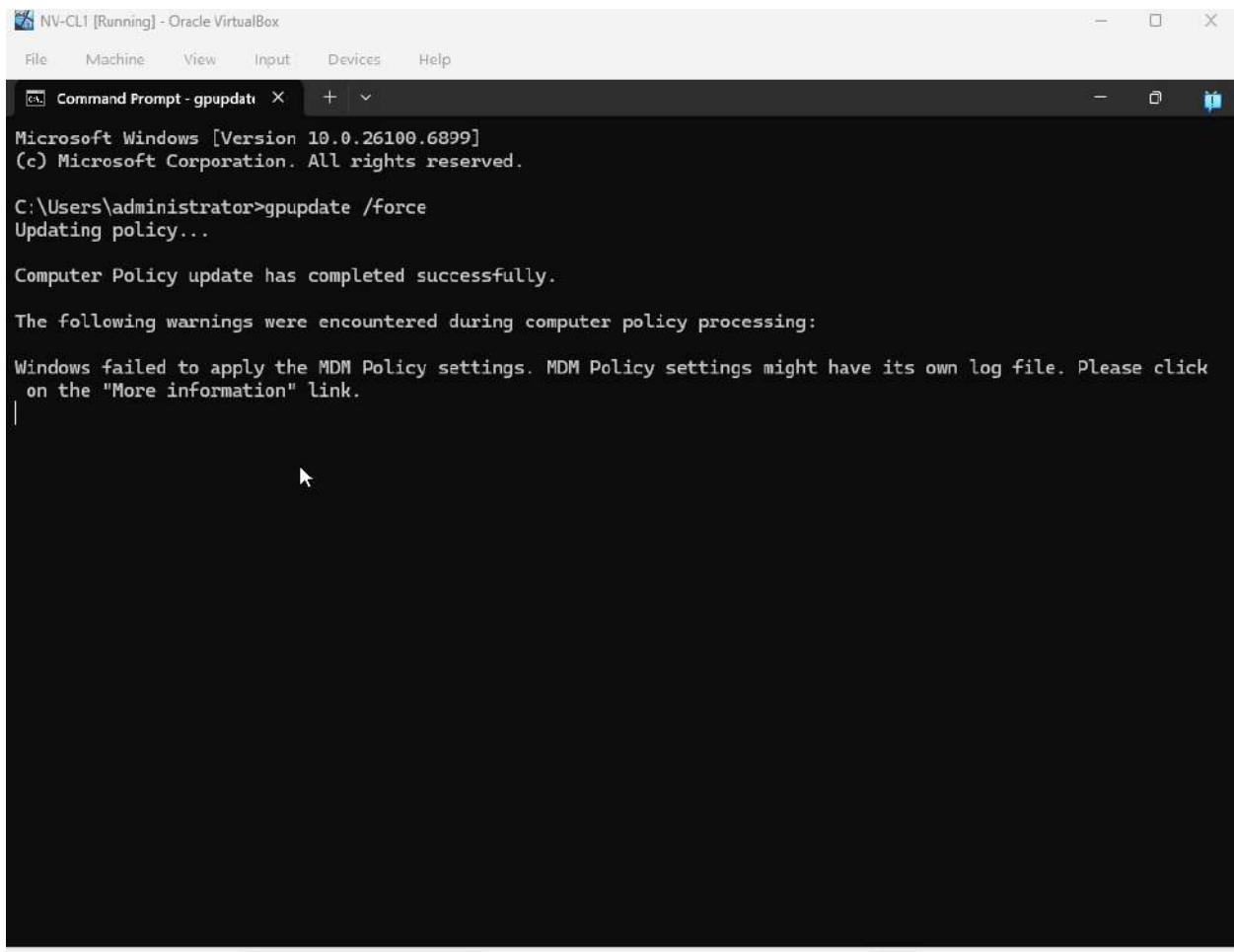
1. Evidence 1: Screenshot showing MDM user scope set to All in Intune.



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-CLI [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 Right Ctrl

This screenshot shows a Windows Command Prompt window titled 'NV-CLI [Running] - Oracle VirtualBox'. 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 taskbar at the bottom shows various pinned icons and the current date and time (5:19 PM, 12/1/2025).

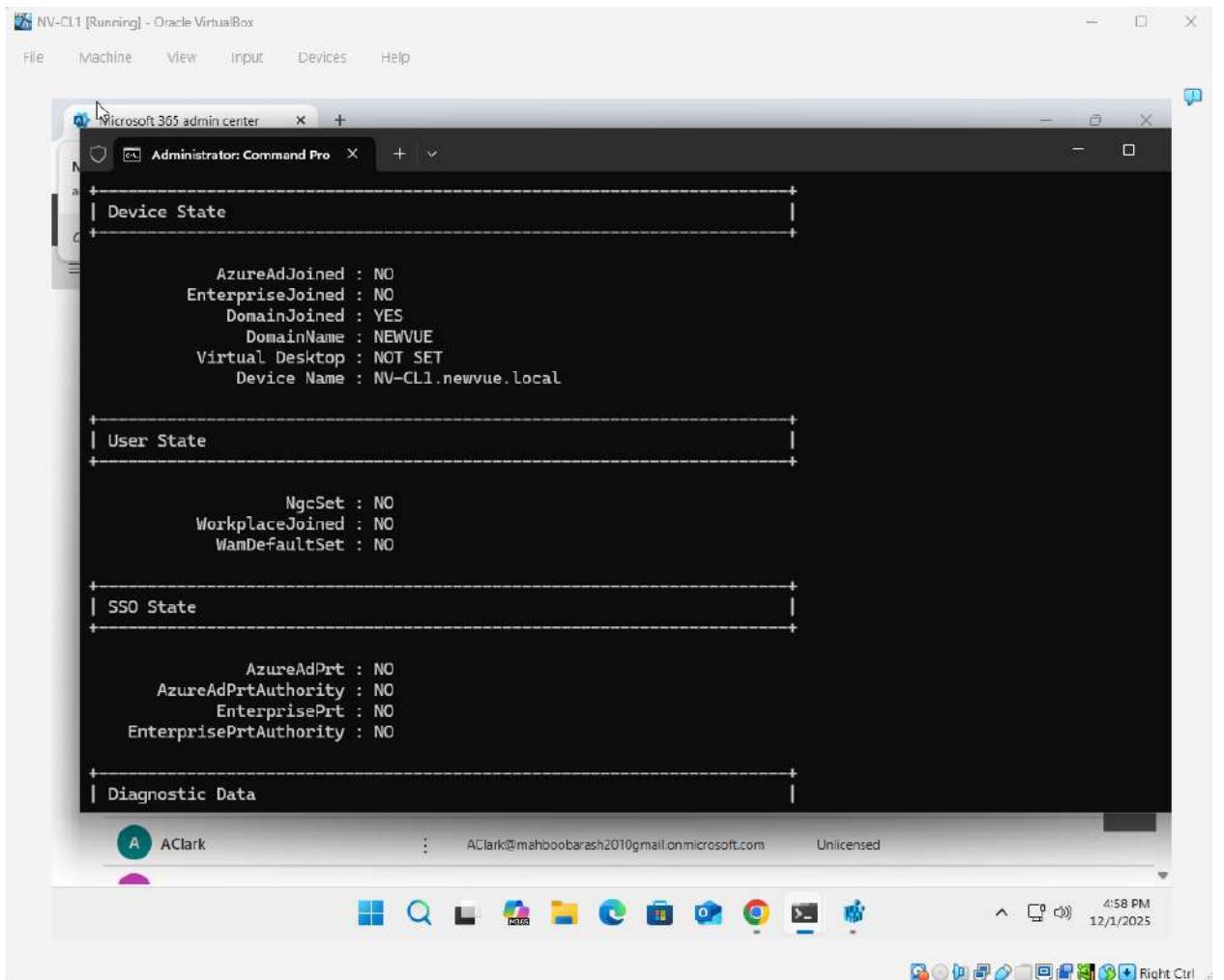
Task 2— Hybrid Azure AD Join & Intune Enrollment Validation

(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

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



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Pro" running in Oracle VirtualBox. The command "dsregcmd /status" has been run, displaying the following output:

```
+-----+  
| Device State |  
+-----+  
| AzureAdJoined : NO  
| 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 |  
+-----+
```

The output shows that the device is successfully joined to Azure Active Directory (DomainJoined: YES) and is managed by Intune (EnterprisePrt: NO, EnterprisePrtAuthority: NO). The user account AClark is listed at the bottom of the screen.

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 menu is visible, showing various sections like Home, Devices, and Agent ID (Preview). The main content area is titled "Devices | All devices". It displays a table with one device entry:

Name	Enabled	OS	Version	Join type	Owner	MDM	Security settings m...	Compliant	Registered %
NV-CLI	Yes	Windows	10.0.26100.0584	Microsoft Entra reg...	Vivian Goshwary	Microsoft Intune	Microsoft Intune	Yes	11/26/2025, 4:40

The table has a header row with columns: Name, Enabled, OS, Version, Join type, Owner, MDM, Security settings m..., Compliant, and Registered %. There is one device listed under the "All devices" section. The device is named "NV-CLI", is enabled, runs on Windows, has version 10.0.26100.0584, joined via Microsoft Entra registration, owned by Vivian Goshwary, managed by Microsoft Intune, and is compliant. The registration date is 11/26/2025, 4:40.

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

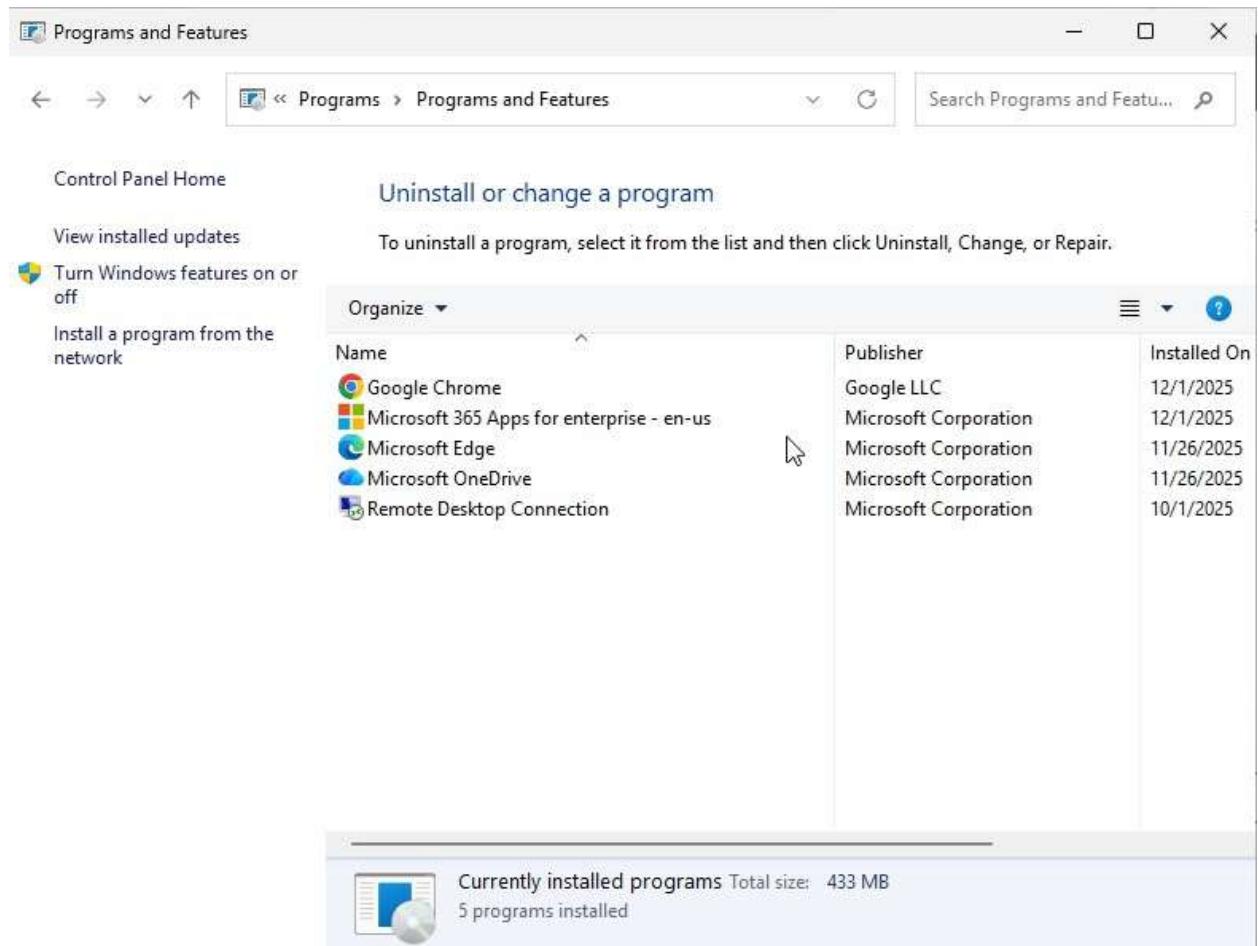
Microsoft 365 Apps were deployed to NV-CLI using Intune application management. This demonstrated cloud-based application delivery and modern software deployment workflows.

Required Evidence

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

The screenshot shows the Microsoft Intune Admin Center interface. The left sidebar includes Home, Dashboard, All services (with sub-options like Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support), and a DevTest - Microsoft Entervision tab. The main content area is titled 'Add Microsoft 365 Apps' under 'Windows apps'. It has tabs for 'App suite information' (selected), 'Configure app suite', 'Assignments', and 'Review + create'. The 'App suite information' section shows the name 'Microsoft 365 Apps for Windows 10 and later' and a description 'Microsoft 365 Apps for Windows 10 and later'. The 'Configure app suite' section contains various configuration options: 'Apps to be installed as part of the suite' (Office), '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 services for Microsoft Search in Bing' (Yes), 'Apps to be installed as part of the suite' (1 language (0 selected)), and 'Default file format' (Office Open Document Format). The 'Assignments' section shows a table with columns Group mode, Group, Status, Filter mode, and Filter, with a single entry for 'Required'. 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 area is titled "Windows 10/11 compliance policy" (Windows 10 and later). It displays tabs for Basics, Compliance settings, Actions for noncompliance, Assignments (selected), and Review + create. Under "Included groups", there is a table with one row: "All users" (Status: Active, Group Members: None, Filter mode: None, Edit filter, Remove). 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" with a table showing "Groups" (Status: Active, Group Members: None, Remove).

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 area is titled "NV-CLI | Device compliance". The navigation bar shows Home > Devices > Overview > Windows > Windows devices > NV-CLI. The left sidebar under "Manage" has sections for Properties, Monitor, Device inventory, Hardware, Discovered apps, Device compliance (selected), Device configuration, App configuration, Recovery keys, User experience, Group membership, Managed Apps, Filter evaluation, Enrollment, and Remediations (preview). The main table lists two items:

Policy name	Logged In user	State	User email	Last contacted
Compliance policies	arash@mahboobbarash2010@gmail.onmicrosoft.com	Compliant		12/01/2025, 04:47
Default Device Compliance Policy	arash@mahboobbarash2010@gmail.onmicrosoft.com	Compliant		12/01/2025, 04:47

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 (selected), 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. Key information shown includes:

- Device name: NV-CLI
- Management name: arash_Windows_12/1/2023_11:50 PM
- Ownership: Personal
- Serial number: VirtualBox-68461012-57ea-45bc-94ad-3d93644e7b1e
- Phone number: ---
- Device manufacturer: Innotek GmbH
- Primary user: Arash.malboorah
- Enrolled by: Arash.malboorah
- Compliance: Compliant
- Operating system: Windows
- Device model: VirtualBox
- Last check-in time: 12/1/2023, 4:47:10 PM
- Remote assistance: Not configured

Below this, there is a 'Device actions status' table with columns Action, Status, Date/Time, and Error, showing '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 shows the registry path: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\Browser. The right pane displays a table of registry keys with columns Name, Type, and Data.

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 for creating an update ring. 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 four tabs: Basics (checked), Update ring settings (checked), Assignments (checked), and Review + create (highlighted in blue). 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: Microsoft product updates (Allow), Windows drivers (Allow), 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 (No), Set feature update uninstall period (2 - 60 days) set to 10, Servicing channel (General Availability channel), User experience settings (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), and Use deadline settings (Not configured). The "Assignments" section includes "Included groups" with entries for "All devices" (Status: Active, Group Members: None) and "All users" (Status: Active, Group Members: None). The "Excluded groups" section shows "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 includes links for 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 has tabs for Basics (selected), Update ring settings (selected), Assignments, and Review + create. Under 'Update settings', there are sections for Microsoft product updates (Allow/Block), Windows drivers (Allow/Block), Quality update deferral period (days: 2), Feature update deferral period (days: 7), Upgrade Windows 10 devices to Latest Windows 11 release (Yes/No), Set feature update uninstall period (2 - 60 days: 10), Enable pre-release builds (Enable/Not Configured), and Select pre-release channel (Windows Insider - Release Preview). Under 'User experience settings', there are sections 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), Option to check for Windows updates (Enable/Disable), Change notification update level (Use the default Windows Update notifications), Use deadline settings (Allow/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).

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

The screenshot shows the Microsoft Intune Device Overview page for a device named NV-CL1. The left sidebar includes links for Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, and Groups. The main content area displays the device's name, management name (arash_Windows_12/1/2025_11:50 PM), ownership (Personal), serial number (VirtualBox-68451012-57ea-45bc-84ad-3d93644e7b1e), phone number (+**), and manufacturer (innotek GmbH). A right-click context menu is open over the device, showing options like Update Windows Defender security intelligence, BitLocker key rotation, Rename device, New remote assistance session, Locate device, Pause config refresh, Run remediation (preview), and Not configured.

Device name: NV-CL1
Management name: arash_Windows_12/1/2025_11:50 PM
Ownership: Personal
Serial number: VirtualBox-68451012-57ea-45bc-84ad-3d93644e7b1e
Phone number: +**
Device manufacturer: innotek GmbH

Primary user: [User icon]
Enrolled by: [User icon]
Compliance: [Icon]
Operating system: [Icon]
Device model: [Icon]
Last check-in time: [Icon]
Remote assistance: Not configured

Update Windows Defender security intelligence
BitLocker key rotation
Rename device
New remote assistance session
Locate device
Pause config refresh
Run remediation (preview)

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 navigation includes Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area shows the path: Home > Devices | Overview > Windows | Windows devices > NV-CLI. The title bar says "NV-CLI | Hardware". The left sidebar under "Hardware" has several collapsed sections: Discovered apps, Device compliance, Device configuration, App configuration, Recovery keys, User experience, Group membership, Managed Apps, Filter evaluation, Enrollment, and Remediations (preview). The "Hardware" section is expanded, showing detailed system information. The "System" section includes fields like Name (NV-CLI), Management name (arash_Windows11_12/1/2025_11:50 PM), and Intune Device ID (424355ca-ab7-4f8e-b700-605fbec07214). The "Operating system" section shows Windows 10/11 Professional (64) with a security patch level of 70.17.0B. The "Storage" section lists Total storage space (76.17 GB) and Free storage space (43.48 GB). The "System enclosure" section shows Manufacturer (innotek GmbH), Model (VirtualBox), Processor Architecture (x64), and Phone number (empty). The "Network details" section includes fields for Ethernet MAC (00007878A98), ICCID, Wi-Fi IP address, Wi-Fi subnet ID, and Wind IPv4 address (10.0.2.18). The "Network service" section shows Enrollment date (12/1/2025 11:50:16 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 (Agents, Reports, Users, Groups, Tenant administration, Troubleshooting + support), and Devices (Devices, Apps, Endpoint security). The main content area is titled "NV-CLI | Device compliance" and displays the "Overview" section. A search bar and filter options are at the top. Below is a table with two items:

Policy name	Logged In user	State	User email	Last contacted
Compliance policies	arash@mahboobarash2010@gmail.onmicrosoft.com	Compliant		12/01/2025, 04:47
Default Device Compliance Policy	arash@mahboobarash2010@gmail.onmicrosoft.com	Compliant		12/01/2025, 04:47

The "Manage" section on the left has a sub-menu under "Device compliance" which includes: Device configuration, App configuration, Recovery keys, User experience, Group membership, Managed Apps, Filter evaluation, Enrollment, and Remediations (preview).