

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.

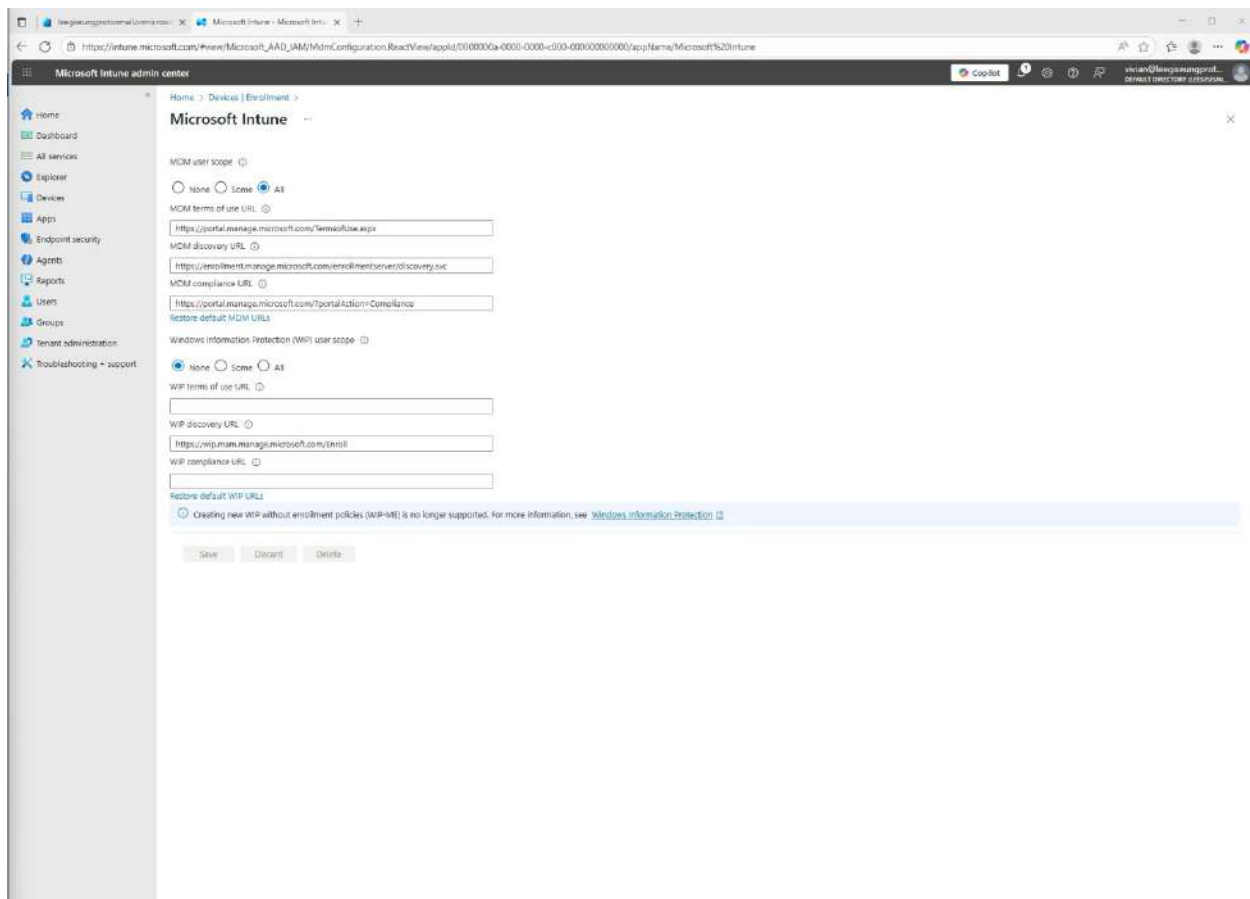
Section 2: Implementation & Verification Evidence

Task 1- Automatic Intune Enrollment Configuration (15 pts)

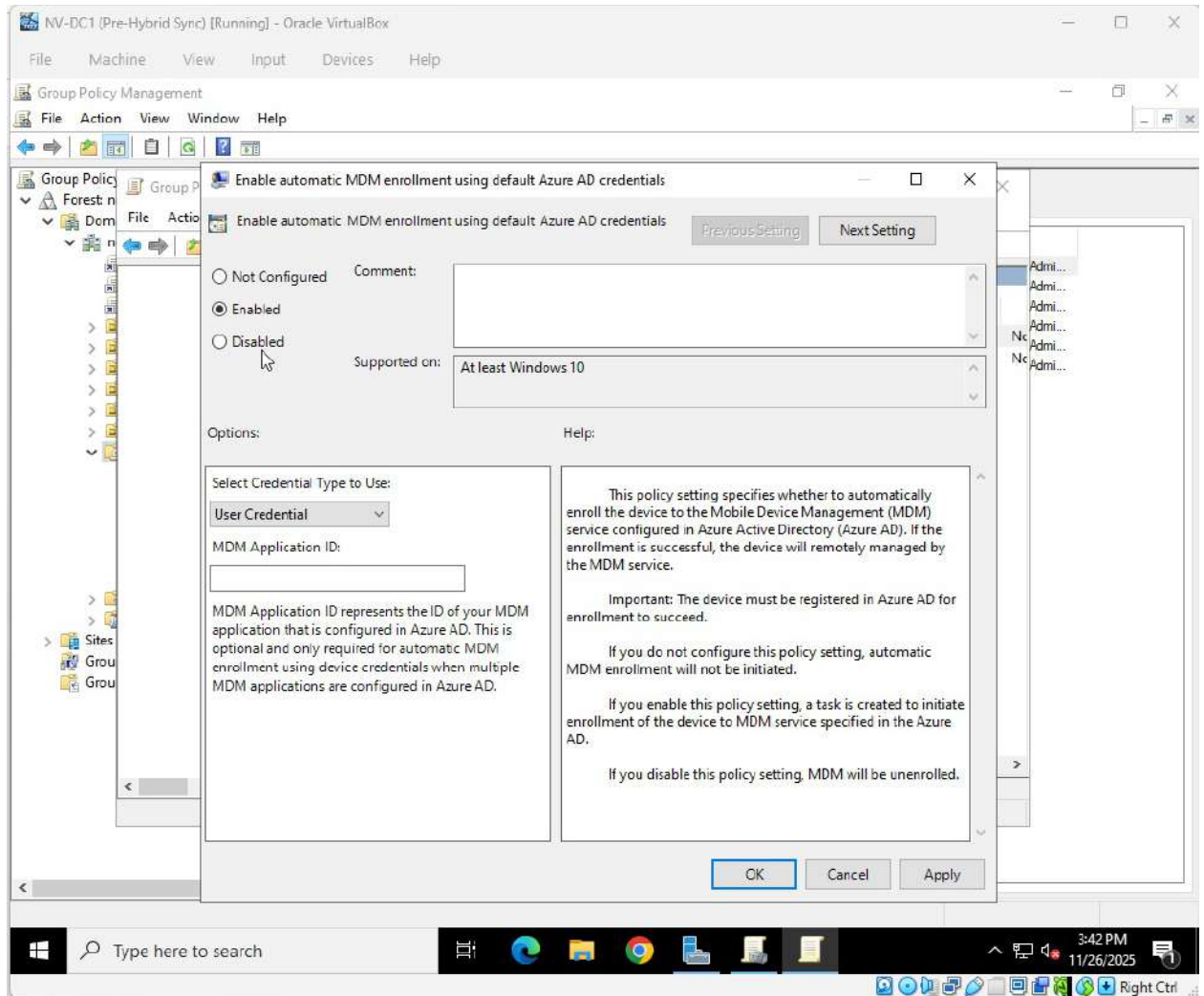
A configuration policy was created to ensure that domain-joined devices are automatically enrolled into Intune during Hybrid Azure AD Join. This step ensures seamless onboarding of corporate Windows endpoints into the organization's cloud management environment.

Required Evidence

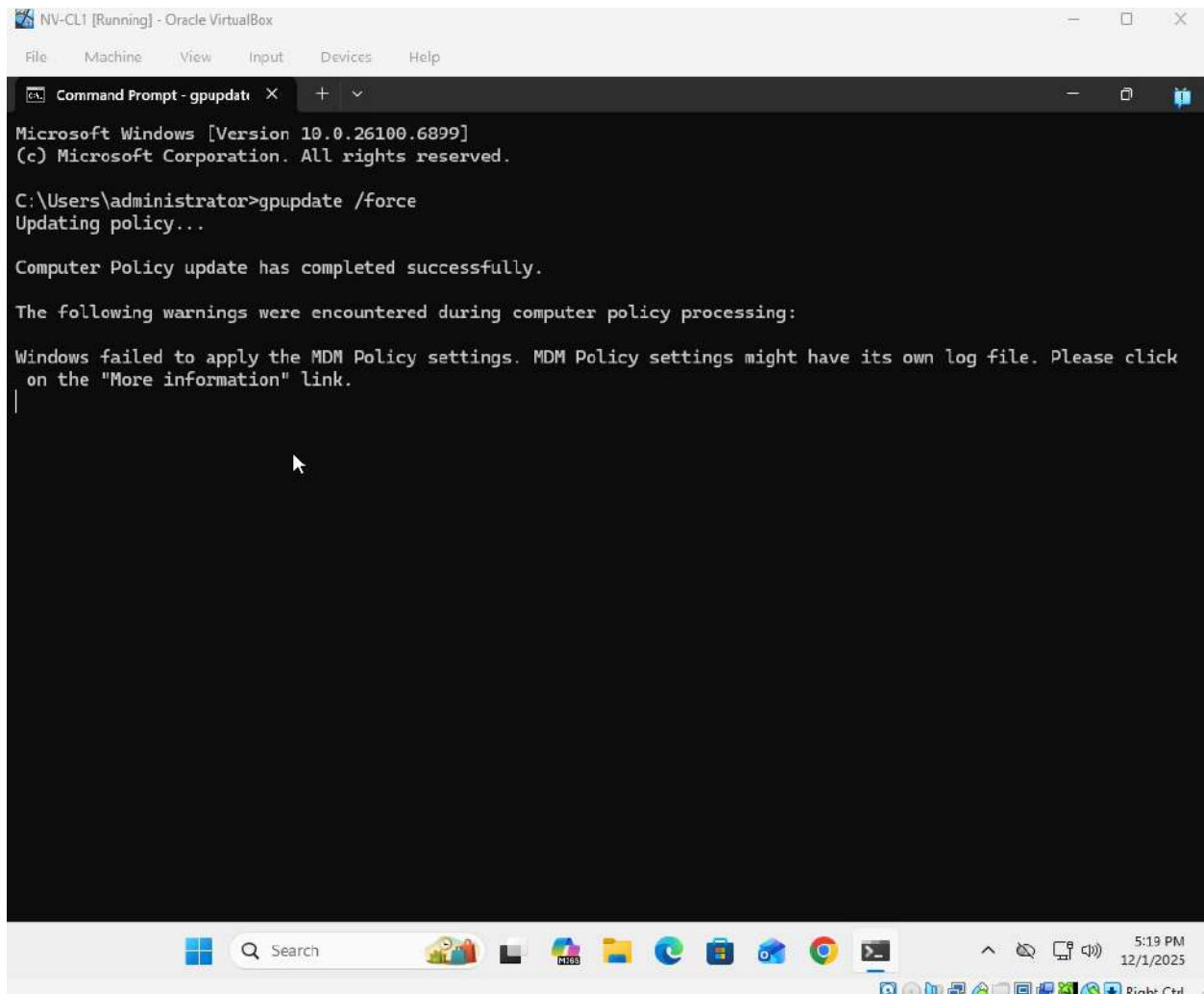
1. **Evidence 1:** Screenshot showing MDM user scope set to **All** in Intune.



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.



The screenshot shows a Windows Command Prompt window titled "Command Prompt - gpupdati" running the command `gpupdate /force`. The output indicates that the policy update was successful, but there were warnings regarding MDM Policy settings. The window is running inside an Oracle VM VirtualBox environment, as indicated by the title bar "NV-CLI [Running] - Oracle VirtualBox". The taskbar at the bottom shows various application icons and the system clock displaying 5:19 PM on 12/1/2025.

```
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.
```

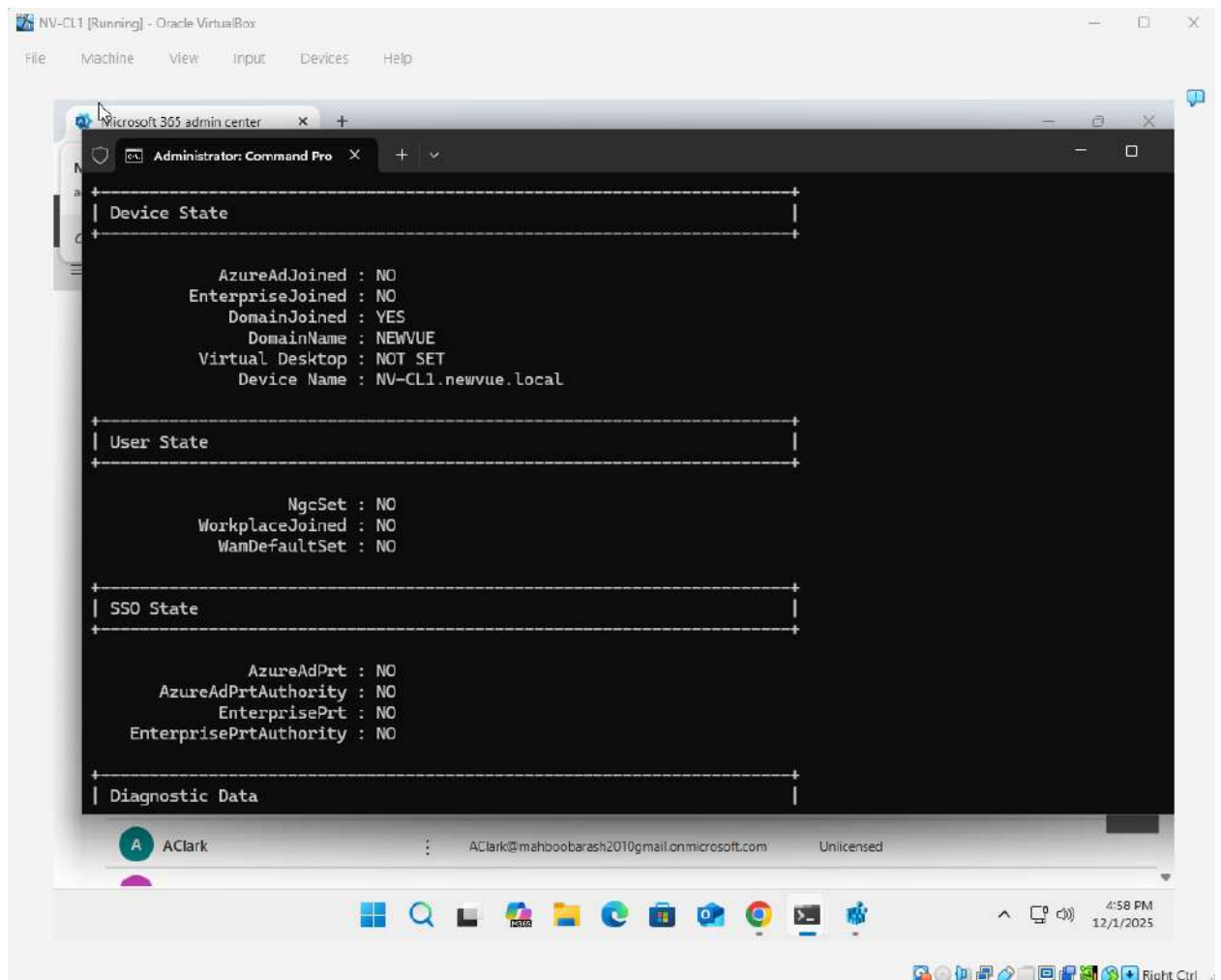
Task 2— Hybrid Azure AD Join & Intune Enrollment Validation

(10 pts)

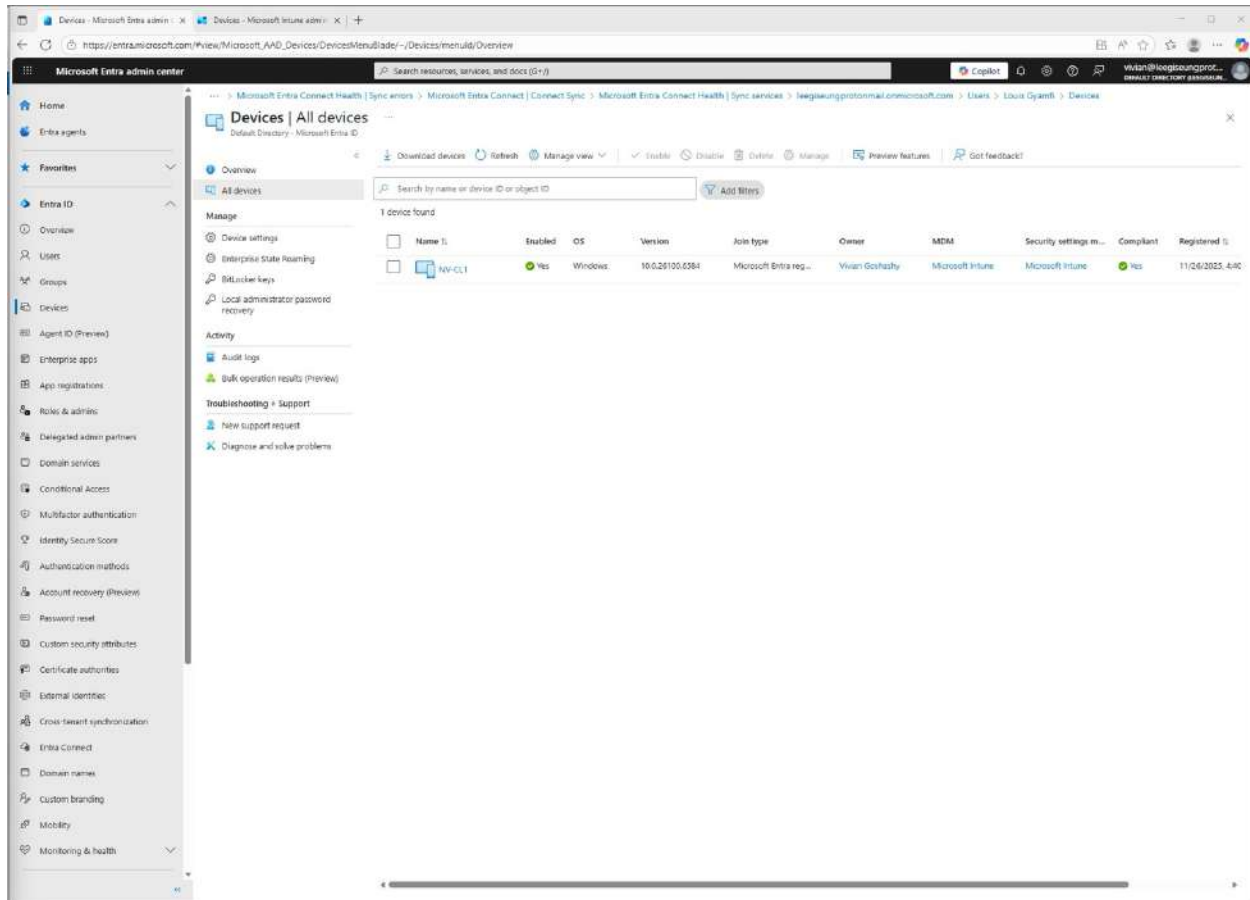
NV-CLI was validated to confirm successful Hybrid Azure AD Join and Intune MDM enrollment. These verification steps ensure the device is correctly registered and managed through cloud policies.

Required Evidence

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



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

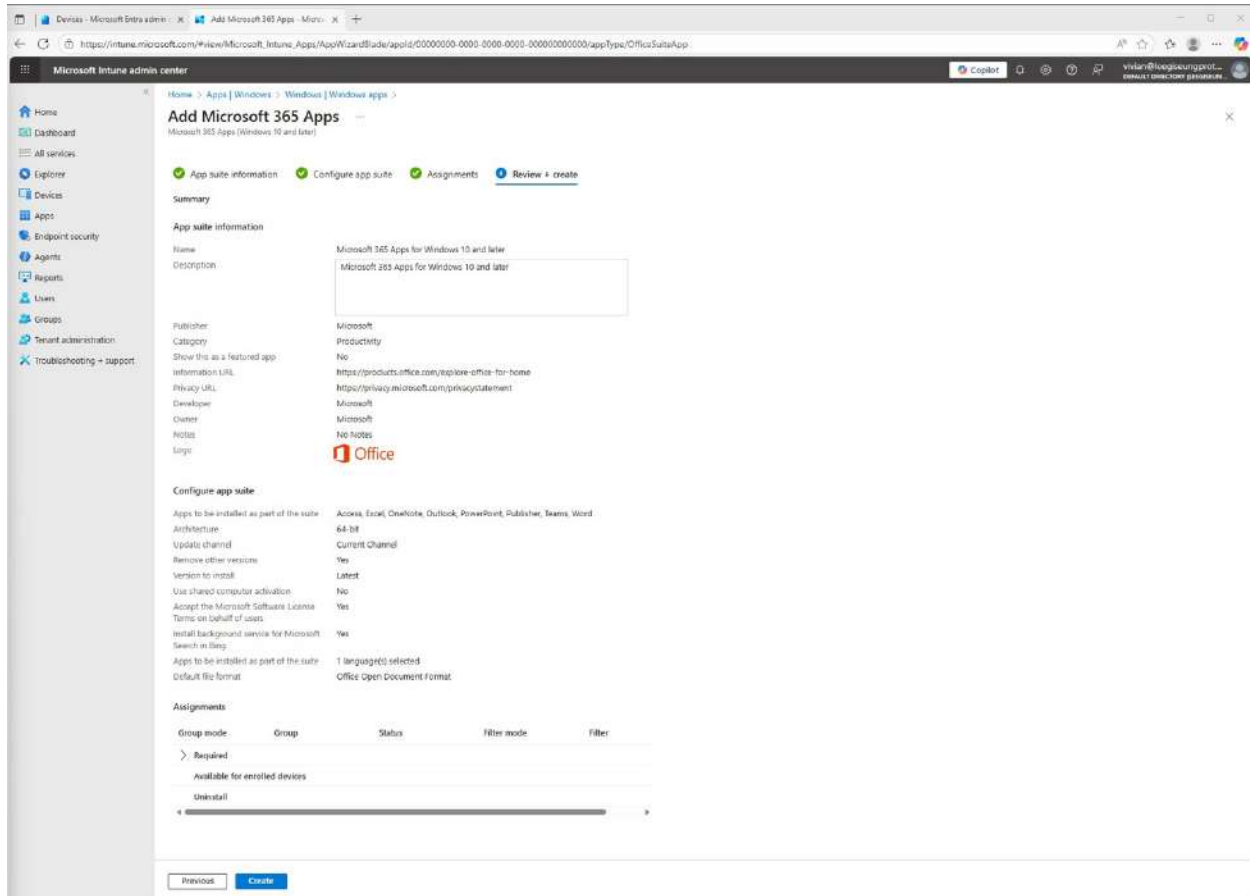


Task 3— Microsoft 365 (Office) Deployment (10 points)

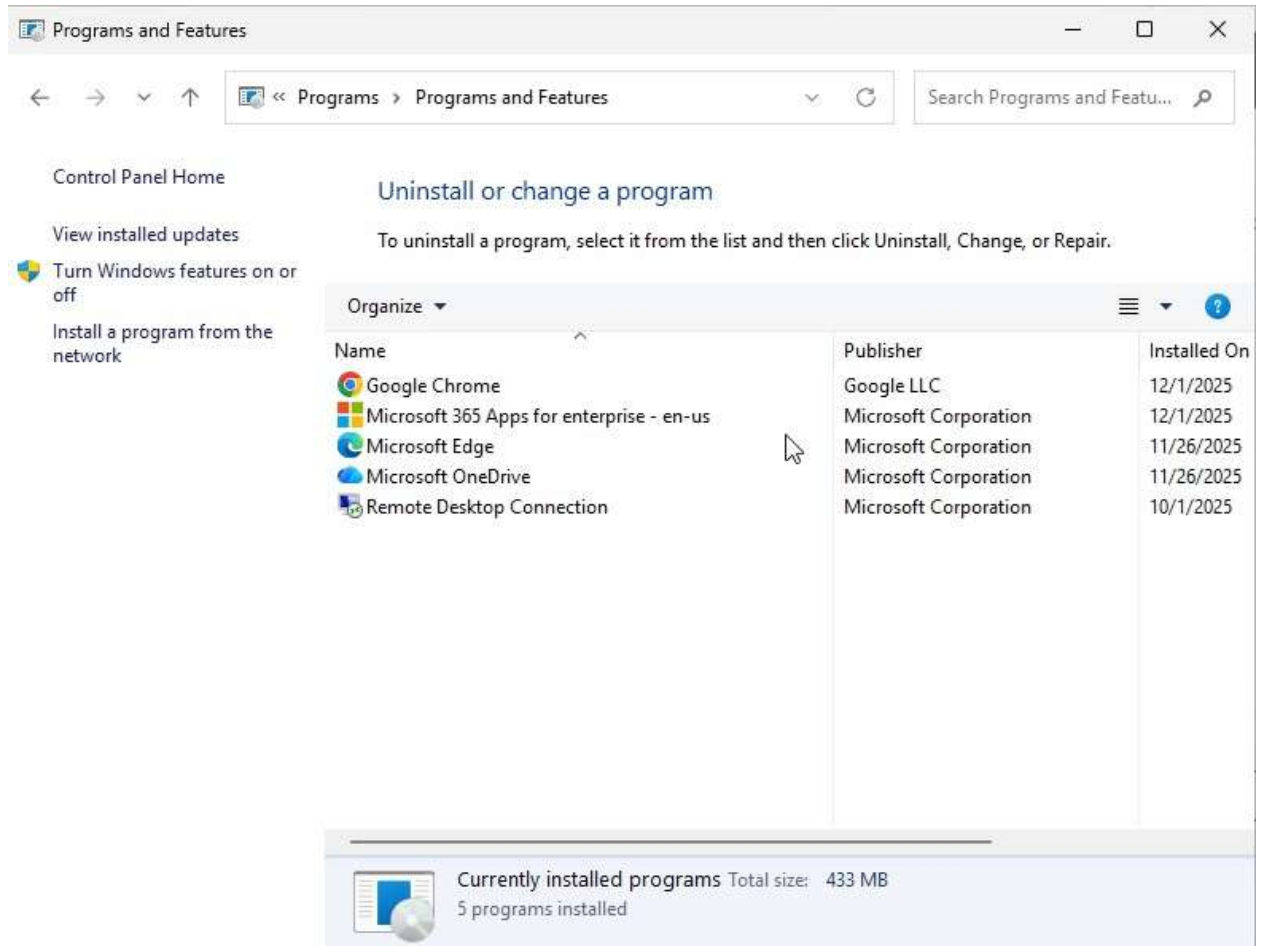
Microsoft 365 Apps were deployed to NV-CLI using Intune application management. This demonstrated cloud-based application delivery and modern software deployment workflows.

Required Evidence

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



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



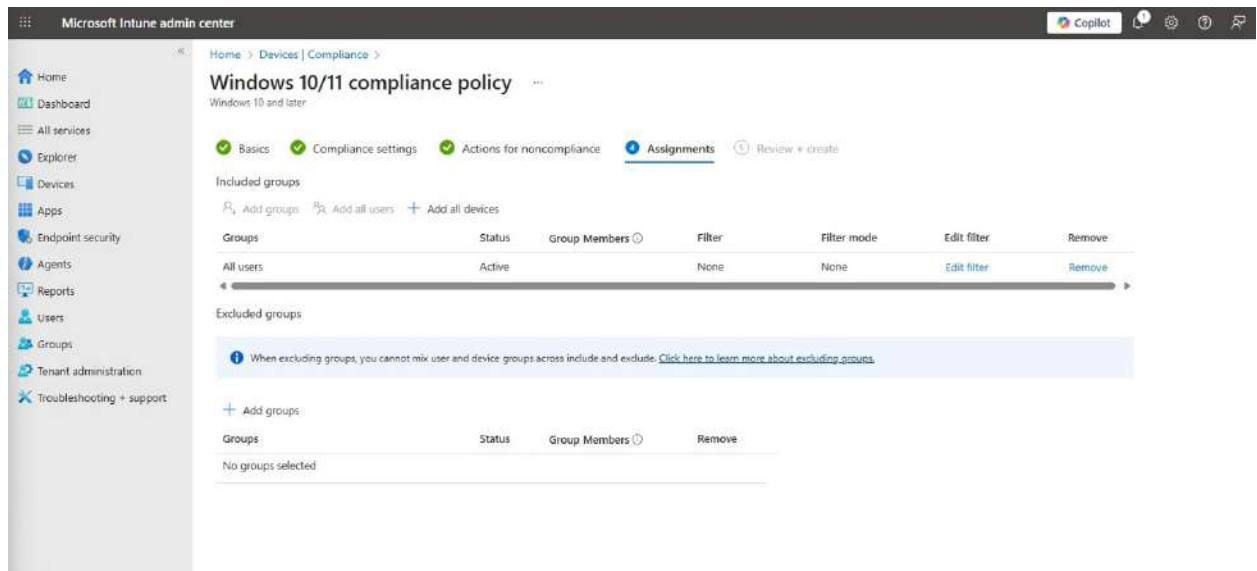
Task 4 - Compliance Policies & Security Baseline (20 pts)

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

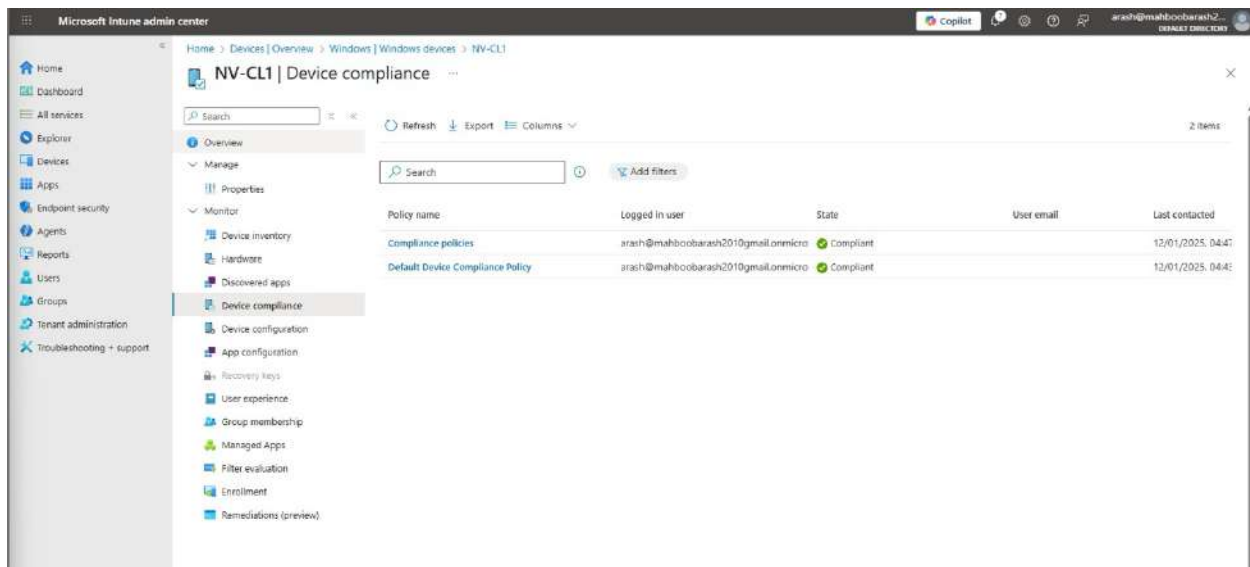
These policies demonstrate how cloud-managed devices are governed by centralized controls.

Required Evidence

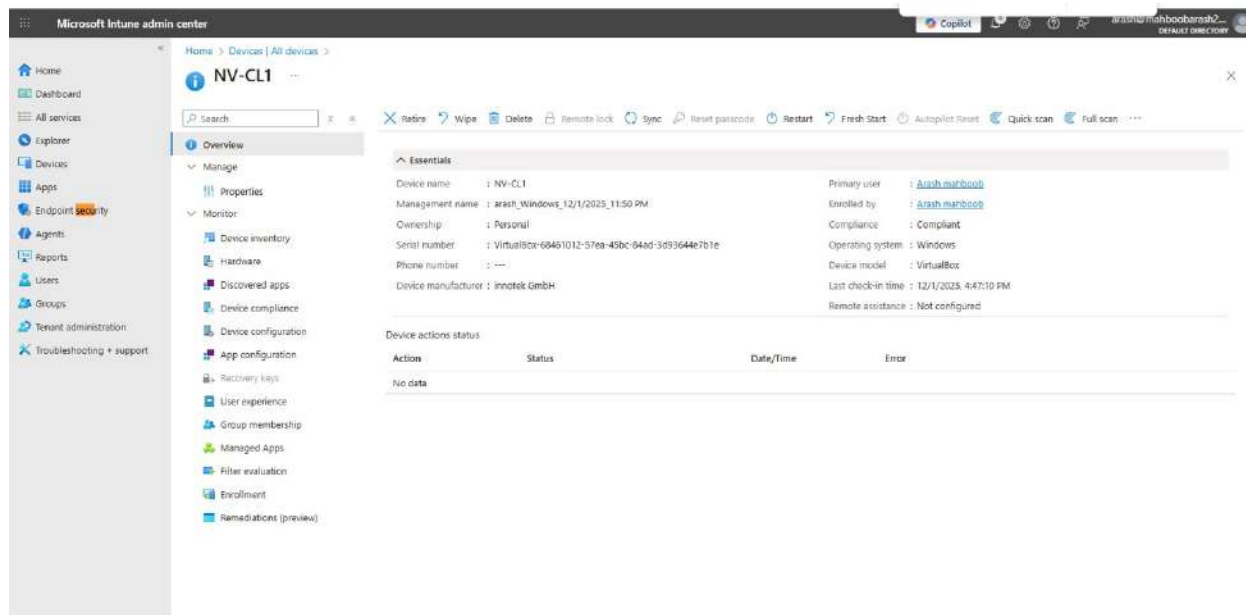
8. Evidence 8: Screenshot of the Compliance Policy assignment.



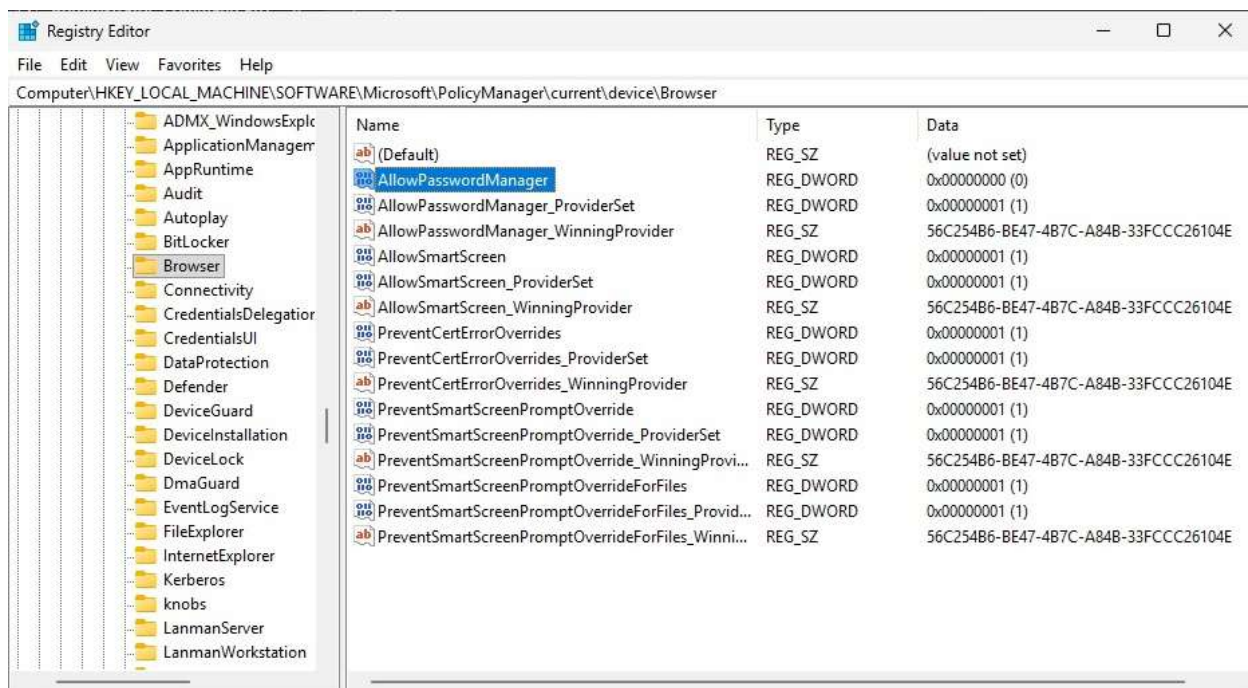
9. Evidence 9: Screenshot of NV-CLI compliance status.



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



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



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 displays the Microsoft Intune admin center interface. The left sidebar contains navigation links: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Create Update ring for Windows 10 and later' and includes a breadcrumb trail: Home > Devices | Windows > Windows | Windows updates >. Below the title, there are four tabs: Basics (selected), Update ring settings, Assignments, and Review + create. The 'Basics' tab shows the following configuration details:

- Summary**
- Basics**
 - Name: NewVue - Update Ring
 - Description: No Description
- Update ring settings**
 - Update settings:
 - Microsoft product updates: Allow
 - Windows drivers: Allow
 - Quality update deferral period (days): 2
 - Feature update deferral period (days): 7
 - Upgrade Windows 10 devices to Latest Windows 11 release: No
 - Set feature update uninstall period (2 - 60 days): 10
 - 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

Below the settings, the 'Assignments' section is visible, showing 'Included groups' and 'Excluded groups' tables.

Group	Status	Group Members	Filter
All devices	Active		None
All users	Active		None

The 'Excluded groups' section shows 'No results'.

Task 6 - Remote Device Actions (10 pts)

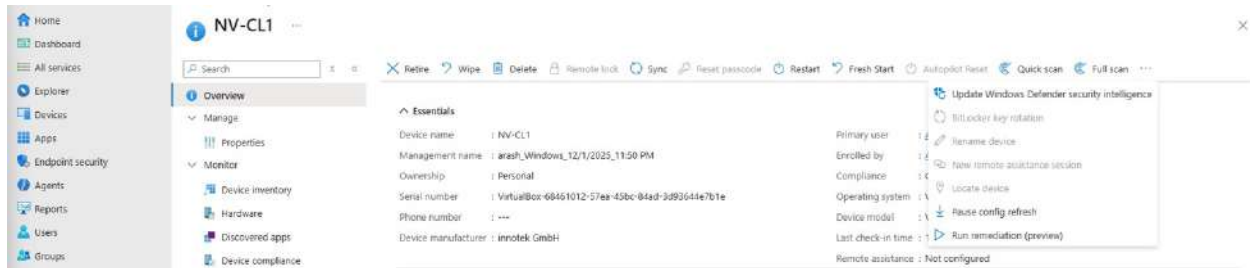
Basic remote management actions were executed from the Intune Admin Center, such as Sync or Restart. This demonstrates remote control and cloud-based management capabilities.

Required Evidence

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

The screenshot displays the Microsoft Intune admin center interface. The left sidebar contains navigation links: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Create Update ring for Windows 10 and later' with a breadcrumb trail: Home > Devices > Windows > Windows updates > Create Update ring for Windows 10 and later. Below the title, there are four tabs: Basics (checked), Update ring settings (active), Assignments, and Review + create. The 'Update ring settings' tab is expanded, showing various configuration options. Under 'Update settings', there are sections for 'Update settings' and 'User experience settings'. The 'Update settings' section includes: 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 (Not configured), and Select pre-release channel (Windows Insider - Release Preview). The 'User experience settings' section includes: 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 (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).



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-CL1.

The screenshot displays the Microsoft Intune admin center interface. The left-hand navigation pane includes links to 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-CL1 | Hardware' and shows a search bar and a list of management actions: Overview, Manage (Properties, Monitor), Device inventory, Hardware (selected), Discovered apps, Device compliance, Device configuration, App configuration, Recovery keys, User experience, Group membership, Managed Apps, Filter evaluation, Enrollment, and Remediations (preview). The hardware details are organized into several sections:

- System:**
 - Name: NV-CL1
 - Management name: arash_Windows_12/1/2025_11:50 PM
 - Intune Device ID: 424355ca-aab7-4f5e-b760-605f8ec8f214
 - Microsoft Entra Device ID: 424355ca-aab7-4f5e-b760-605f8ec8f214
 - Serial number: VirtualBox-68461012-57aa-45bc-84ad-3d93644e7b1e
 - Enrollment profile
- Operating system:**
 - Operating system: Windows
 - Operating system version: 10.0.26100.6599
 - Operating system language: en-US
 - Operating system edition: Pro
 - Operating system SKU: Windows 10/11 Professional (48)
 - Security patch level
- Subscription:**
 - Status
- Storage:**
 - Total storage space: 75.17 GB
 - Free storage space: 43.48 GB
 - Total physical memory
- System enclosure:**
 - IMB
 - MID
 - Manufacturer: innotek GmbH
 - Model: VirtualBox
 - Processor Architecture: x64
 - Phone number
 - TPM Version
 - TPM manufacturer ID
 - TPM manufacturer version
 - System management BIOS version
- Network details:**
 - Subscriber carrier
 - Cellular technology
 - Wi-Fi MAC: 080027878A98
 - Ethernet MAC
 - ICCID
 - Wi-Fi IP address
 - Wi-Fi subnet ID
 - Wired IPv4 address: 10.0.2.18
- Network service:**
 - Enrolled date: 12/1/2025 3:50:16 PM

Evidence 16: Screenshot of the Device Compliance overview for NV-CL1.

Microsoft Intune admin center

Home > Devices > Overview > Windows > Windows devices > NV-CL1

NV-CL1 | Device compliance

Search Refresh Export Columns 2 items

Overview

Manage

Monitor

- Device inventory
- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Recovery keys
- User experience
- Group membership
- Managed Apps
- Filter evaluation
- Enrollment
- Remediations (preview)

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