MDM Using Microsoft Intune and Entra ID Lab

Nelson R. Acevedo | Cybersecurity Student

Introduction:

This project demonstrates centralized device management on the cloud. In this project, I applied mobile device management (MDM) by using Microsoft Intune and Microsoft Entra ID.

Project Goals:

The goals of this project were:

- Manage Windows devices by using Microsoft Intune.
- Enroll Devices on Microsoft Entra ID.
- Implement and configure policies.
- Simulate a real organization.
- Implement MDM in the cloud.
- Manage and troubleshoot policies and enrollment issues.
- Implement BitLocker and other security measures.
- Deploy apps for compliant devices.
- Implement conditional access.

Tools:

- Microsoft Intune (MDM)
- Microsoft Entra ID (Cloud identity)
- VM Ware (VM creation and management)
- Windows 11 client (enrollment, apps and policies testing).

Environment Design:

Organization Name: NelCorp.

Virtual Machines:

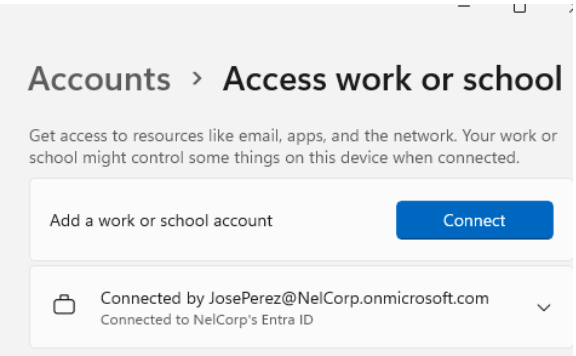
- User– Windows 11 (Entra ID-Joined)

Implementation Steps:

1. Tenant setup
2. User and group creation
3. Device enrollment
4. Configuration profile enforcement
5. Compliance policy configuration
6. Conditional Access policy
7. App deployment
8. Monitoring and validation

Tenant setup:

The user VM was joined to Entra ID by using a user's credentials, and then was added to the device group.



Screenshot - User after enrolling in Entra ID.

Users and Groups:

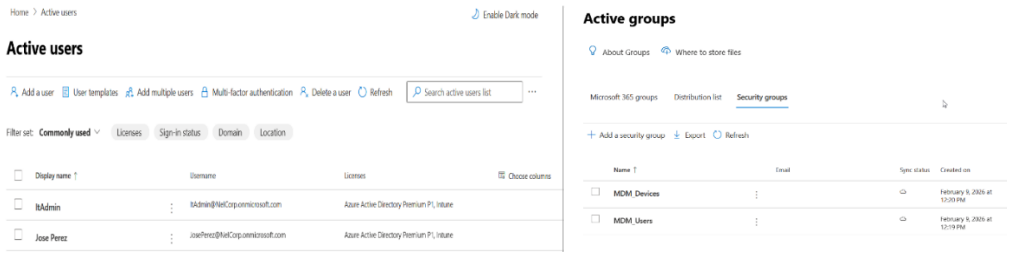
Users:

- Jose Perez → normal user
- ItAdmin → user with administrator privileges

Groups:

- **MDM_Users**
- **MDM_Devices**

This configuration allows to control users' and devices' policies and security measures in a more organized way.



Screenshots - Active users and groups

Compliance policy configuration:

- Require Bitlocker
- Require Code Integrity
- Require encryption of data storage on device
- Require a password with high complexity

If a device doesn't meet these requirements is marked as noncompliant and won't have access to deployed apps and other resources. This ensures that all company devices meet basic requirements.

Security Controls Implemented:

- BitLocker enforcement
- Password complexity requirements
- USB storage blocking
- Conditional access requiring compliant devices

A configuration profile enforcement policy was created to make sure all this was automatically applied.

Conditional Access Policy:

I created a conditional Access Policy in Entra ID to ensure that only compliant devices with multifactor authentication could connect to Entra ID. This prevents unauthorized users and devices with poor security configurations from accessing applications and resources.

Policy configuration:

- **Name:** Require Compliant Device for MDM User
- **Grant access:** Require compliant device and multifactor authentication.
- **Assign:** MDM_Users

Security Impact:

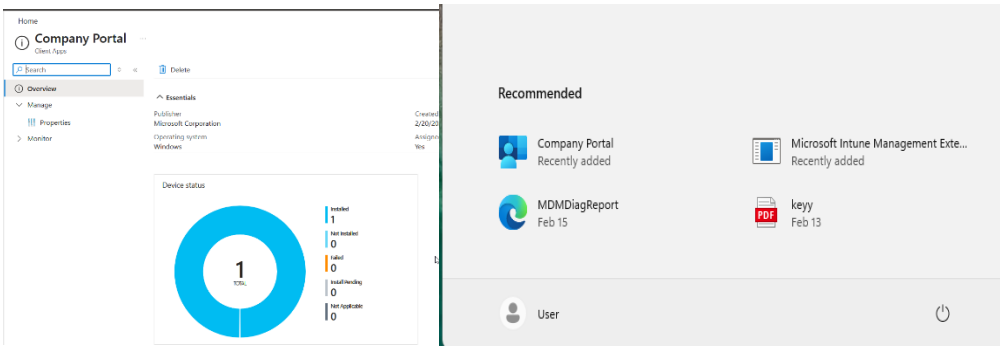
- Prevents unauthorized device access
- Blocks non-compliant devices from accessing cloud apps
- Enforces encryption at rest
- Reduces risk of data exfiltration

App Deployment:

Application Type

- **Platform:** Windows 10/11
- **App type:** Microsoft Store app (new)
- **Assignment type:** Required
- **Target group:** Device group

⚠️ Initially, the installation behavior was set to User, while the app was assigned to a device group which caused an error. However, after some trouble shooting the app was able to work and was automatically installed in the client device.



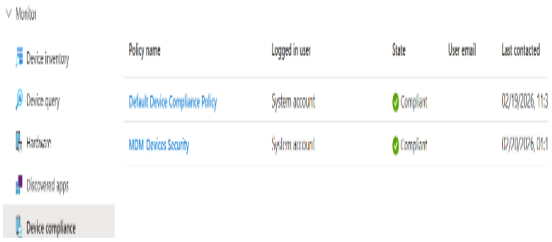
Screenshots – App status in Intune and App installed in client device

---

Testing and Validation:

- **Device Compliance Verification** I temporarily disabled BitLocker to simulate non-compliance. After activating it again the device became compliant again. This was verified within Microsoft Intune under **Devices → Compliance**.
- **Application Deployment Test:** The Microsoft app was successfully installed on the client devices, and this was confirmed on Intune as well by checking the app status.
- **Conditional Access Enforcement Test:** The policy required a compliant device and multi-factor authentication. When attempting access, authentication requirements were enforced

according to the policy configuration. This confirmed that access control was dependent on compliance status and identity verification.



Screenshot – Showing the device is compliant in Microsoft Intune

---

Challenges Encountered:

- **The device was Azure AD Registered but not Azure AD Joined (MDM Enrolled).:**
    - 🚨 Challenge: Device Enrollment Error — When the device was only registered the device allowed most policies to apply, but app deployment did not function correctly.
    - 🛠️ Fix: I had to disconnect the device and connect it again to be enrolled instead of register.

App Deployment Misconfiguration:

- 🚨 Challenge: The application installation initially failed because the installation behavior was configured for users while the app assignment targeted a device group.
- 🛠️ Fix: After reviewing the assignment configuration and aligning it with a device-based deployment model, the issue was resolved.

These challenges made me realize the importance of the assignment of security groups, the configurations, and structured troubleshooting.

Lessons Learned:

- **Compliance vs. Configuration Policies:** Compliance policies only check if the device is compliant while configuration policies automatically apply or ask you to apply certain configurations when you log in in the device.
- **Cloud-Based Endpoint Security:** Microsoft Intune and Entra ID provide centralized visibility and control over endpoint security posture, enabling secure remote device management.
- **Conditional Access Dependency:** Conditional access policies depend completely in compliance policies and configurations of the device. A bad or good configuration in the compliance policies decides who and what devices have access to our services in the cloud.
