Steps For Intune Deployment

Step 1 - Set up Intune

This step focuses on setting up Intune and getting it ready for you to manage your user identities, apps, and devices.

- Add users and groups in Microsoft Entra ID
- Assign Intune licenses to users

Step 2 - Add and protect apps

Protect apps and data across both company-owned and personal devices

- For enrolled devices:
  Create a list of required apps and assign them during enrollment.
  Apply App Protection Policies to secure sensitive apps.

- For non-enrolled (personal) devices:
  Use App Protection Policies to safeguard company data.
  Enable Multi-Factor Authentication (MFA) for added security.

Step 3 - Check for compliance and turn on Conditional Access

Protect your organization's data by allowing access only from secure and compliant devices.

- Create compliance policies to define security rules that devices must meet.
- Assign these policies during device enrollment.
- Enable Conditional Access to ensure only compliant devices can access company resources.

Step 4: Configure Device Features

Ensure all devices are set up securely and consistently to protect organizational data.

- Define a baseline of device and security features (like password settings, encryption, etc.) that must be enabled or blocked.
- Assign configuration profiles to devices during enrollment.

Step 5: Enroll Your Devices

- Enroll devices in Microsoft Intune to manage and secure them.
- Devices must be enrolled to receive compliance rules, app policies, configuration settings, and security features.
- Admins set up enrollment policies based on device types (Windows, Android, iOS, macOS, Linux).
- During enrollment, devices get a secure MDM certificate to connect with Intune.
- Enrollment can be manual (by users) **or** automated depending on your setup.

Ensure devices are securely enrolled so Intune can manage and protect them.