Intune Application Deployment and Setup of Deployment

Step 1: - Set Up Intune

- Verify that your device types are supported. Then, initiate your Intune tenant, add users and groups, allocate the appropriate licenses, and complete other initial setup steps.
- Establish administrative roles and define user scopes for better management and control.

Step 2: - Add, Configure, and Secure Applications

- For devices that will be enrolled in Intune, define a baseline of essential applications and assign these app configurations during the enrollment process.
- For devices that are not enrolled in Intune, apply app protection policies combined with MultiFactor Authentication (MFA) to enhance security.
- You can also integrate Microsoft Defender for Endpoint for improved threat protection on managed apps.

Step 3: - Utilize Compliance and Conditional Access

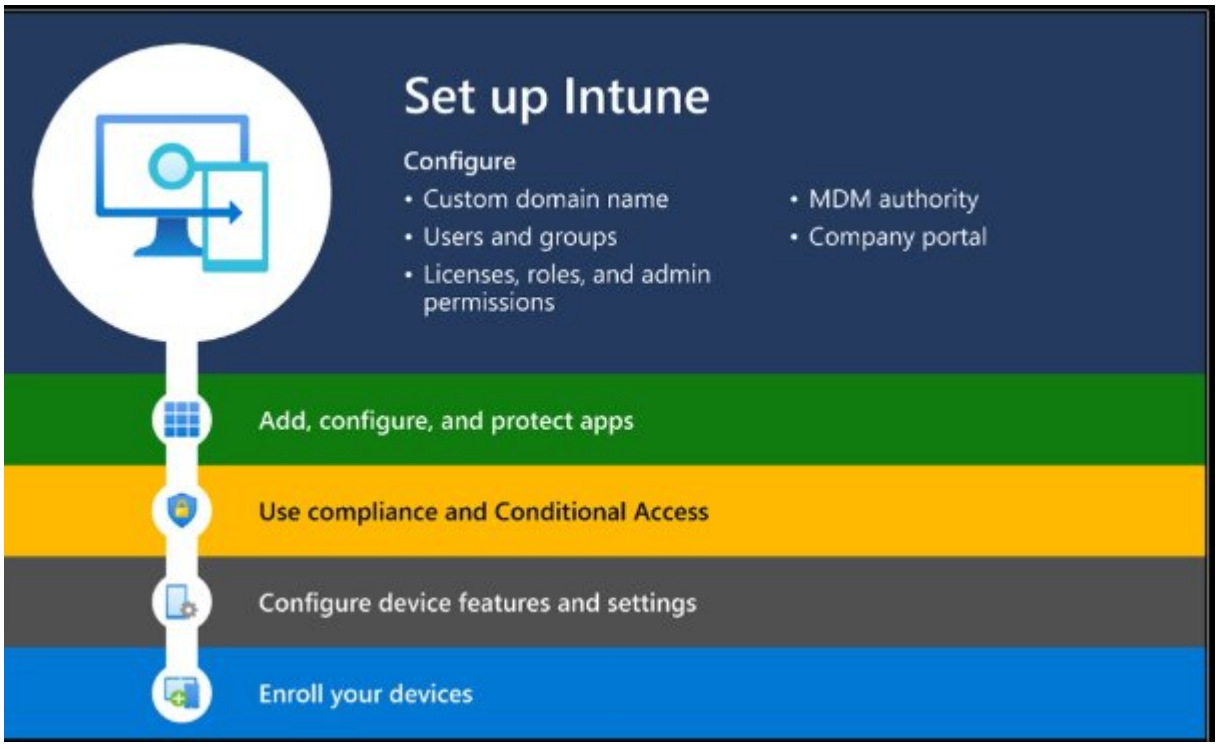
- Set up a compliance policy baseline to ensure that all devices meet organizational security and configuration standards. Assign these policies at the time of enrollment.
- Implement Conditional Access rules to enforce compliance. Only compliant devices should be granted access to organizational resources.
- Using Conditional Access in tandem with compliance policies helps prevent data breaches and ensures secure device access.

Step 4: - Configure Device Features and Policies

- Define and apply a standard configuration for device settings, including security features, password policies, and hardware controls.
- Restrict or allow specific features such as camera, Bluetooth, or USB ports, based on organizational policies.

Step 5: - Device Enrollment

- Enroll your devices into Intune to begin centralized management.
- Devices must be enrolled in Intune to receive the full range of policies including compliance, Conditional Access, app deployment, and security configurations.
- Enrollment can be automated using Autopilot for Windows devices, streamlining setup and configuration for end users.



Deploying Windows Applications Using Intune

1. Preparing Your Application:

a. **Win32 Applications**: For legacy Windows apps, package them using the **Win32 Content Prep Tool** to generate a .intunewin file for deployment.
b. **Microsoft Store Applications**: For apps sourced from the Microsoft Store for Business or Education, no repackaging is required—just configure and deploy.
c. You should also ensure the app has been tested for compatibility across the various device types you plan to support.

2. Adding the Application to Intune:

a. Log in to the **Microsoft Intune Admin Center**
b. Navigate to **Apps > All Apps**
c. Click **Add**, then select the appropriate application type (e.g., Win32, Microsoft Store, etc.)
d. Complete the required fields by uploading your app package or entering details such as the name, publisher, and download URL.

3. Assigning the Application:

a. After the app is added, go to **Apps > All Apps**, and select your newly added app.
b. Click on **Assignments** to choose which **user or device groups** will receive the app.
c. Optionally, set a deadline or availability time for when the app should be installed.

4. Managing Application Deployment:

a. **Deployment Options**: Intune supports a range of deployment methods such as **silent installs**, **required installs**, and **available installs** where users can opt-in via the Company Portal.
b. **Monitoring**: Use the Intune Admin Center to track installation status, failures, and compliance metrics.
c. **App Removal**: You can also **uninstall or retire apps** remotely through the same interface if they are no longer required or need to be updated.
d. Regularly reviewing deployment status helps maintain software compliance and ensures smooth user experience.