**Name**: Saniya Galib Tamboli

**Email**: [saniyagtamboli2412@gmail.com](mailto:saniyagtamboli2412@gmail.com)

**Batch**: DWS\_B5\_25VID2550

**User Id**: 34749

**Date**: 07/08/2025

ASSIGNMENT

1. **Convert a Win32 application installer (.exe) into the .intunewin format:**

Step 1: Download the IntuneWinAppUtil tool

Go to official Microsoft site or search for:

Microsoft Win32 Content Prep Tool (IntuneWinAppUtil)

Or download from Microsoft GitHub Repo

Extract the downloaded ZIP file.

You will get a file named: IntuneWinAppUtil.exe

Step 2: Place the .exe file in a working folder

Create a folder (e.g., C:\IntuneApps) and put:IntuneWinAppUtil.exe

The .exe installer you want to convert (e.g., MyAppInstaller.exe)

Any related install files (if needed)

Step 3: Run the tool via Command Prompt

Open Command Prompt as Administrator.

Navigate to the folder containing the tool:

cd C:\IntuneApps

Run the tool:

IntuneWinAppUtil.exe

You will be prompted to enter:

Source folder: Location of your .exe file (e.g., C:\IntuneApps)

Setup file: Name of your .exe file (e.g., MyAppInstaller.exe)

Output folder: Where to save the .intunewin file (e.g., C:\IntuneApps\Output)

Catalog folder: Press Enter to skip this.

**Example:**

Please specify the source folder: C:\IntuneApps

Please specify the setup file: MyAppInstaller.exe

Please specify the output folder: C:\IntuneApps\Output

Do you want to specify catalog folder (Y/N)? N

After this, it will generate a .intunewin file in the output folder.

**Final Output:**

You will get something like:

MyAppInstaller.intunewin

You can now upload this to Microsoft Intune Admin Center for app deployment.

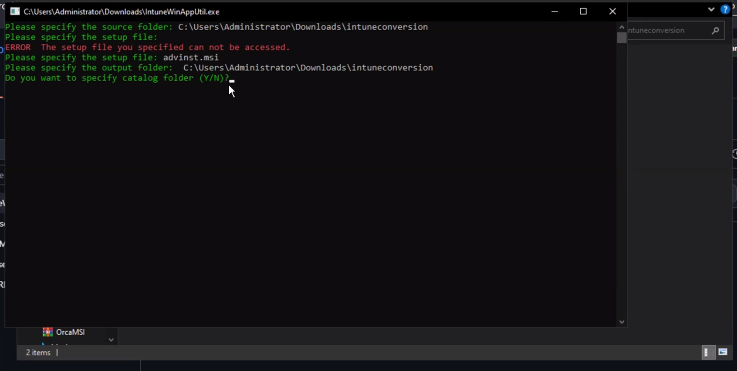


Fig.1. .exe to .intunewin

1. **Process Flow for an Application on Windows client via IME service. (From Polling to detection, to installation, to detection and toast notifications as success/failure):**

1. Polling:

The IME service periodically polls the Microsoft Intune server for new or updated application deployments. This polling maintains the client device in sync with the latest Intune application assignments.

2. Detection:

•Before Installation intune checks detection rules to see if the app is already installed on the device before installation.

•After Installation detection rules are re-evaluated after installation to ensure whether the application is operating as desired.

•Detection rules can be based on registry entries, file presence and process presence.

3. Installation:

If the application is not yet installed on the device, the IME initiates the installation.

• Download and Unpacking: The .intunewin package is downloaded and unpacked into a staging directory on the client device.

• Installer Execution: The admin executes a command from within the Intune portal to install the program, usually msiexec or other similar installers.

• Installation Monitoring: The installation is being monitored; if it takes longer than the timeout, it's a failure.

4. Detection & Notifications:

• Post-Installation Detection: Installation rules are re-evaluated to ensure proper installation of apps.

• Success/Failure Notifications: The system shows toast notifications to notify the user if the application installation was successful or not.

• Toast notifications: Small, graphical (visually appealing) notifications that show the deployment status on the user's screen. Toast notifications are customizable with the text, icon and interactive action.

• Device Reboot: The client device can be restarted after installation by Intune policy to implement changes effectively.

1. **Interactive and Non-Interactive Applications**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Interactive Apps** | **Non-Interactive Apps** |
| User Interaction | Required | Not required |
| GUI | Typically has one | Usually none |
| Purpose | User-driven actions | Background automation |
| Examples | Browsers, media players | Services, update agents |

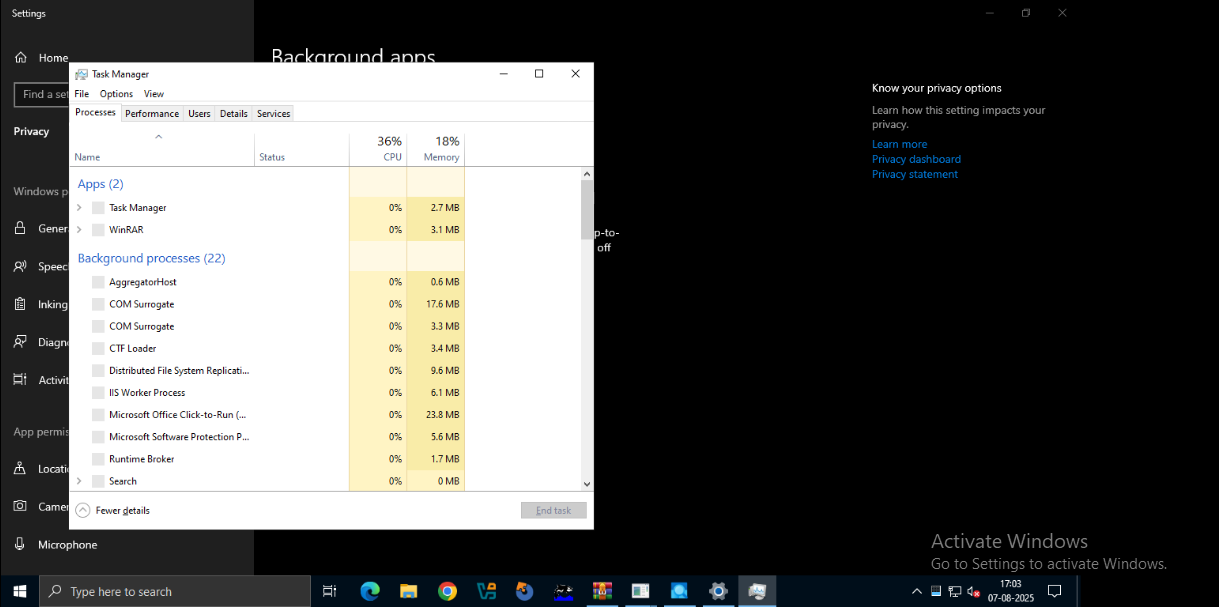


Fig.2. Interactive and Non-Interactive Applications

Interactive applications are designed for direct user interaction through a GUI, while non-interactive applications operate in the background without a user interface, often performing automated tasks.

1. **Required and Available App assignments**

Once app assignments or policy changes are configured in Microsoft Intune, synchronization brings the device up to date to the current settings. It can be triggered manually by admins or users.

1. Sync using Company Portal App

Platform: Windows, Android

Steps:

1. Launch Company Portal.
2. Access Settings and choose Sync.
3. Wait for synchronization to complete.
4. Sync with Intune Admin Center

Platform: All devices.

Steps:

1. Log in to the Intune Admin Center.
2. Go to Devices > All devices.
3. Select a device > Overview > Sync.
4. Confirm the action.
5. Sync in Windows Settings OS: Windows

Steps:

1. Access Settings.
2. Accounts > Allow access to work or school.
3. Select your work account > click Info > choose Sync.
4. Taskbar Sync (Windows)

Steps:

1. Right-click on the Company Portal icon in the tray.
2. Select Sync this device.

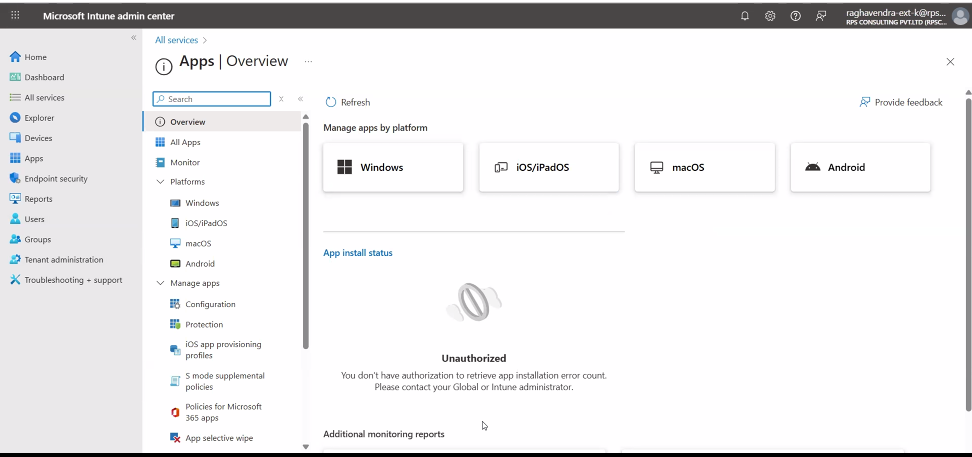


Fig. 3. Intune All Services

Note:

Syncing may take several minutes. Critical for new app rollouts, policy changes, and compliance mandates. Users may be notified by the Company Portal of post-sync changes.

**5**. **Registries with respect to LOB and Win32Apps**:

In Microsoft Intune, the Windows Registry is used to deploy and manage LOB and Win32 applications. It is also a hierarchical Windows configuration information database.

* 1. Windows Registry Role
* Saves application and system settings, preferences and configurations.
* Structures data using keys: folders and values: entries.
  1. LOB Apps
* Line-of-business applications.
* Use the registry to:
  + Save preferences and settings.
  + Maintain app functionality across devices.
  + Allow Intune configuration management.
  1. Win32 Apps
* Traditional Windows desktop applications.
* Depend greatly on the registry for:
  + Track installation progress.
  + Config management.(store config data)
  + Manage app setting.
  1. Intune (manage both LOB and Win32 apps)
* Intune employs registry information to:
  + Ensure an application is installed (according to detection rules).
  + Enforce specific app configurations.
  1. Registry Editing with Caution
* Manual editing must be done carefully.
* Incorrect changes can lead to instability (of system) or app problems.

Windows Registry is critical to LOB and Win32 application management in Intune for detection, validation and configuration control support for secure enterprise app deployment.

**6. Specific Registries with Application GUID which give you the status of Installation/Uninstallation.:**

Windows registry keeps data about installed programs, e.g., unique IDs (GUIDs) for install status or uninstallation verification. This is helpful for Line-of-Business (LOB) and Win32 application management via Microsoft Intune or manual MSI operations.

i. Registry Paths for Apps

* Per-machine installations (all users):

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

* Pre-user installations (specifically for the current user):

HKCU\SOFTWARE\Microsoft\Windows\Uninstall

ii. GUID (Code)

* Every request has a GUID, which is a 32-character unique string.
* The GUID is the sub-key name of the Uninstall registry key.
* It verifies app existence or initiates removal.

iii. Uninstall with GUID:

* Execute Windows Installer (msiexec) with the app's GUID:

msiexec.exe /x {GUID} /QN to uninstall app

* /QN flag specifies silent mode
* /L\*V "C:\\Client-uninstall\\desktop-uninstall.log " directs the uninstallation log to a specified file.

Example:

If {80890A63-01AA-40D3-A2E9-B3E214735151} under the uninstall registry key, remove the application with: msiexec.exe /x {80890A63-01AA-40D3-A2E9-B3E214735151}/QN

iv. Log Files (Optional, Useful)

Event logs validate successful or failed installation or uninstallation.

Important points:

* **Timestamps:**Record the exact time an event occurred, crucial for tracing the sequence of events.
* **Event Types:**Categorize events (e.g., errors, warnings, information, success/failure audits) to prioritize and understand the nature of the event.
* **Severity Levels:**Indicate the importance or impact of an event (e.g., critical, error, warning, informational).
* **Descriptions:**Provide details about the event, including error codes, affected components, and user actions.
* **Event IDs:**Unique identifiers assigned to specific events, allowing for easier searching and

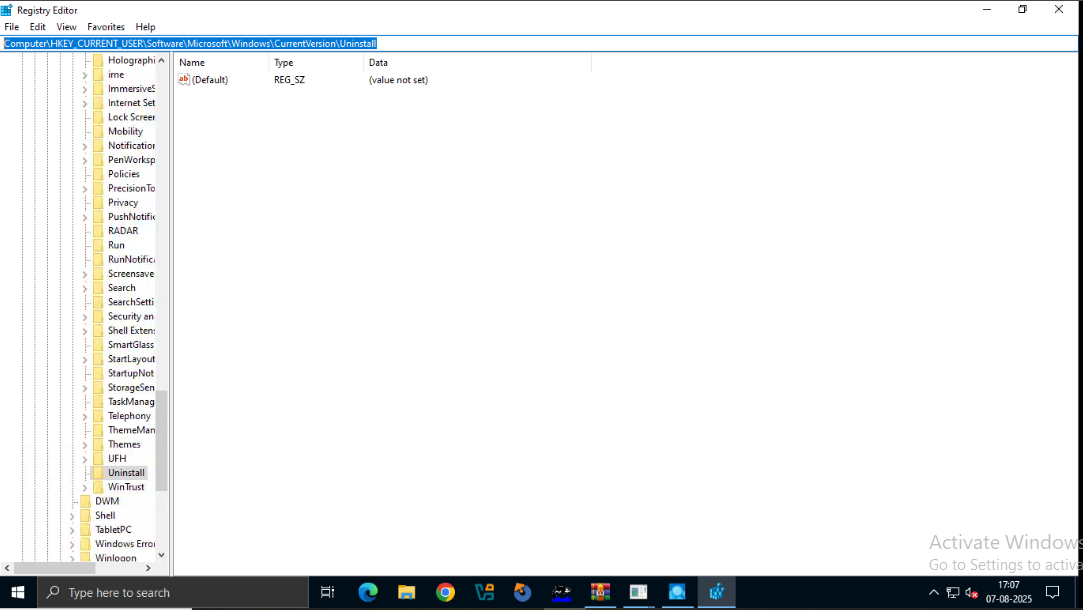


Fig. 4. Registry Key (Uninstall

**7. Microsoft Intune**

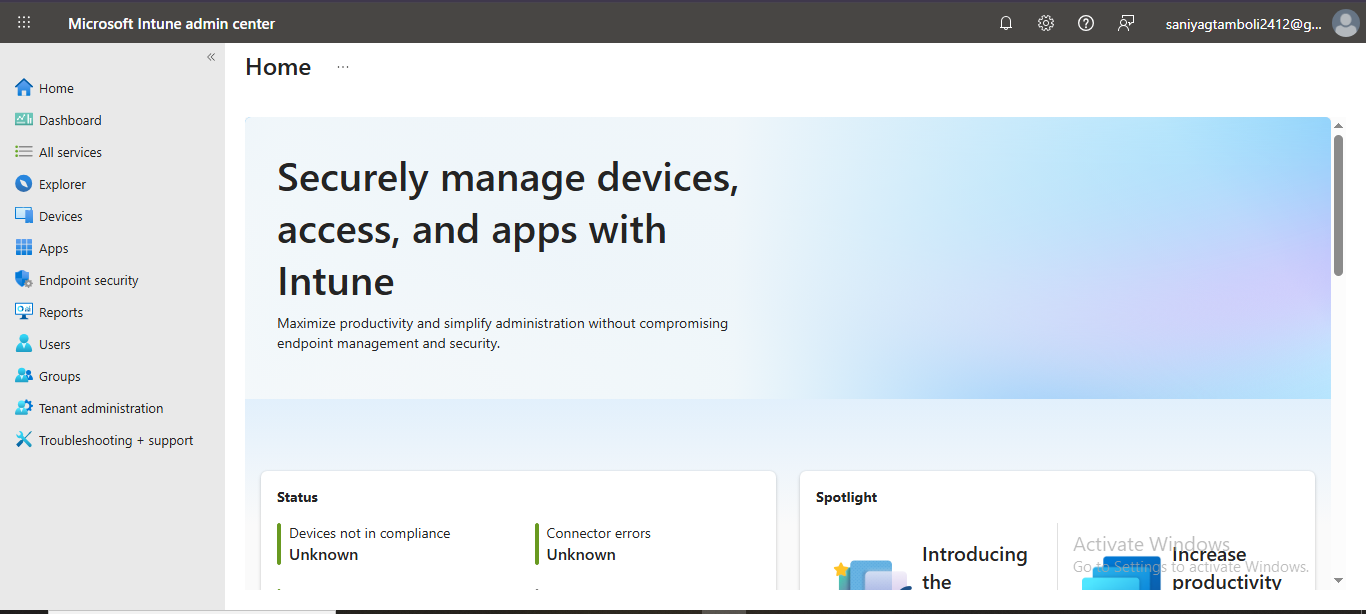


Fig. 5. MS Intune Home Page

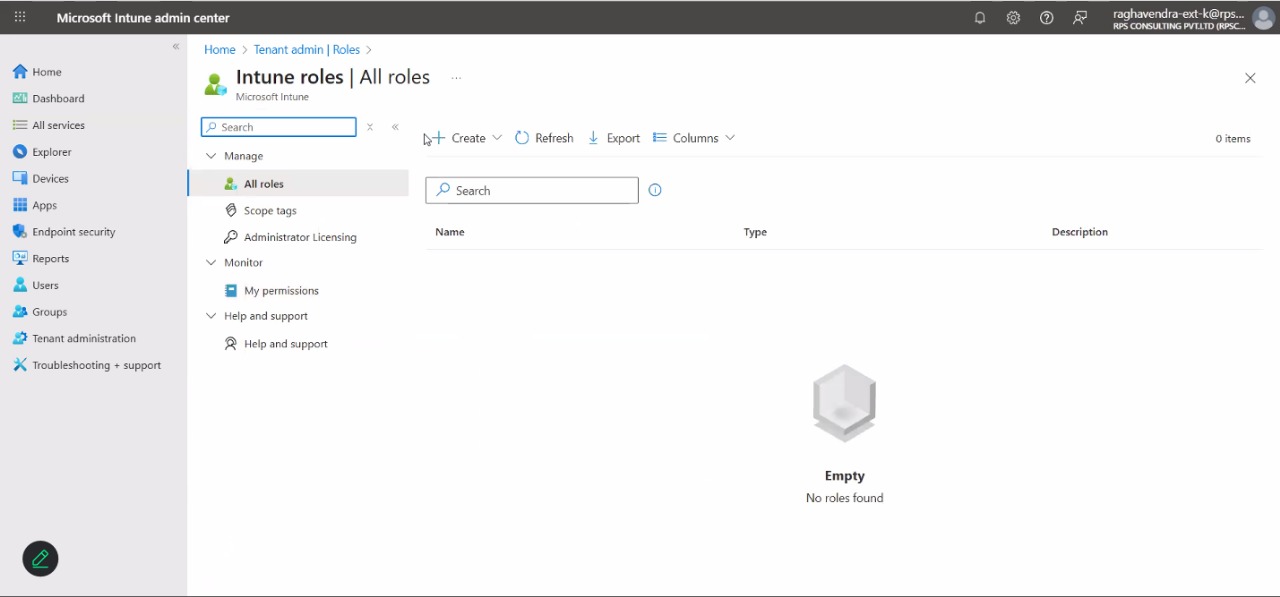


Fig. 6. Intune Roles