**Batch information:**

* **Batch Start Date: 2025-08-04**
* **Batch Name: WiproNGA\_DWS\_B5\_25VID2550**
* **First Name: Seetal**
* **Last Name: Biswal**
* **User Id: 34933**
* **Batch ID: 25VID2550**
* **Assignment Name-** **Interactive and Non-Interactive Applications**
* **Required and Available App assignments**
* **Groups, Dynamic queries, Users**
* **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)**
* **Registries with respect to LOB and Win32Apps**
* **Specific Registries with Application GUID which give you the status of Installation/Uninstallation.**
* **Log File locations**
* **Company Portal**
* **How to Sync once app assignments are done. (Intune Device Sync/ Company Portal Local side Sync)**
* **Breakdown of events in log files.**

**Interactive Applications:**

1. Require user input and interaction (e.g., clicking buttons, entering data).

2. Provide real-time feedback and responses to user actions.

3. Examples:

- Web applications (e.g., online banking, social media).

- Mobile apps (e.g., games, productivity tools).

- Desktop applications (e.g., word processors, image editors).

**Non-Interactive Applications:**

1. Run without direct user interaction or input.

2. Often perform automated tasks or background processes.

3. Examples:

- Server-side applications (e.g., web servers, database servers).

- Batch processing scripts (e.g., data processing, report generation).

- Background services (e.g., antivirus software, system updates).

**Key differences:**

1. User engagement: Interactive apps require user input, while non-interactive apps run autonomously.

2. Response time: Interactive apps respond in real-time, while non-interactive apps may run in the background or at scheduled intervals.

**Required and Available App Assignments:**

In the context of Microsoft Intune or mobile device management (MDM), app assignments can be categorized into two types:

**Required App Assignments:**

1. Mandatory installation: The app is automatically installed on the device.

2. No user choice : Users cannot opt-out of installing the app.

3. Typically used for: Essential business apps, security tools, or compliance-required apps.

**Available App Assignments:**

1. Optional installation: The app is made available to users, but they choose whether to install it.

2. User choice: Users can install or uninstall the app as needed.

3. Typically used for: Productivity apps, departmental apps, or non-essential apps.

Process flow for an application deployment on a Windows client via Microsoft Intune Management Extension (IME) service:

**Step 1: Group Targeting**

1. Create a group: Define a group of users or devices that will receive the application.

2. Dynamic queries: Use dynamic queries to include or exclude devices based on attributes like device type, OS version, or user attributes.

**Step 2: Application Deployment**

1. Assign the application: Assign the application to the targeted group.

2. IME polling: The IME service on the Windows client polls Intune at regular intervals (default is every 8 hours).

**Step 3: Detection**

1. IME detects the policy: When the IME service polls Intune, it detects the application deployment policy.

2. IME checks applicability: The IME service checks if the application is applicable to the device based on requirements and dependencies.

**Step 4: Installation**

1. IME downloads the application: If the application is applicable, the IME service downloads the application installation package.

2. IME installs the application: The IME service installs the application on the device.

**Step 5: Detection (Post-Installation)**

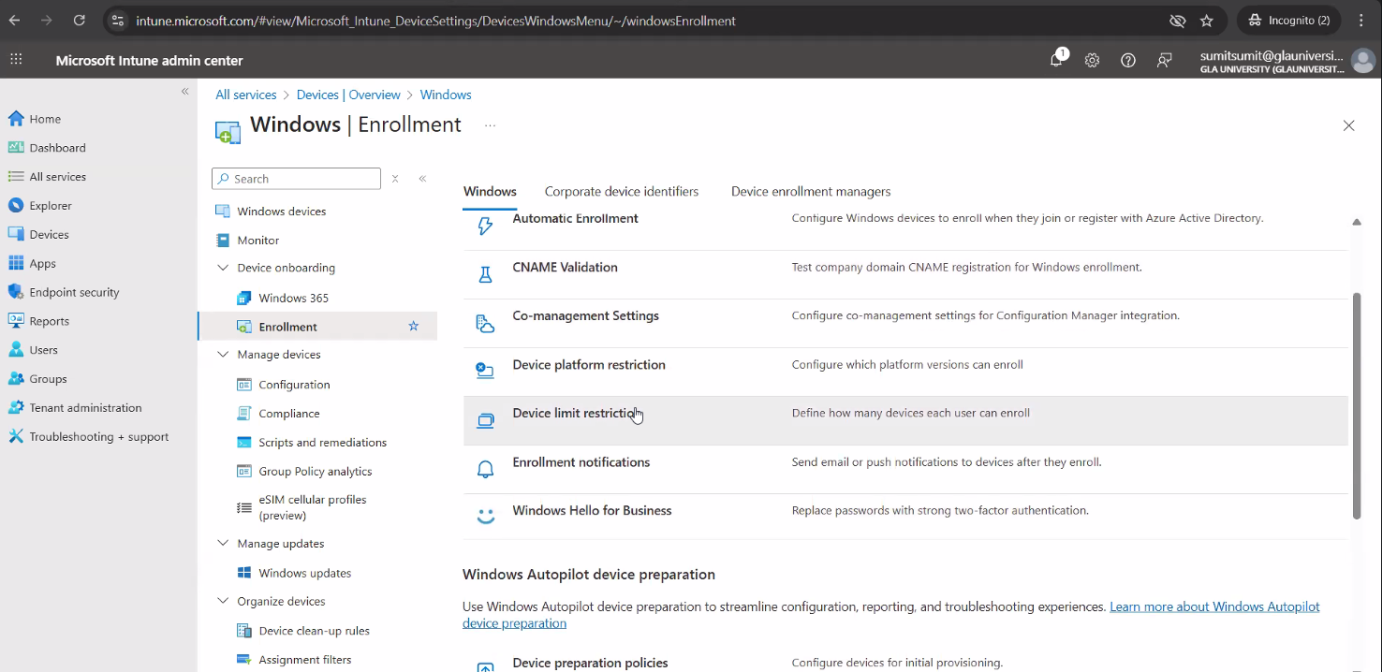
1. IME detects installation status: After installation, the IME service detects the installation status (success or failure).

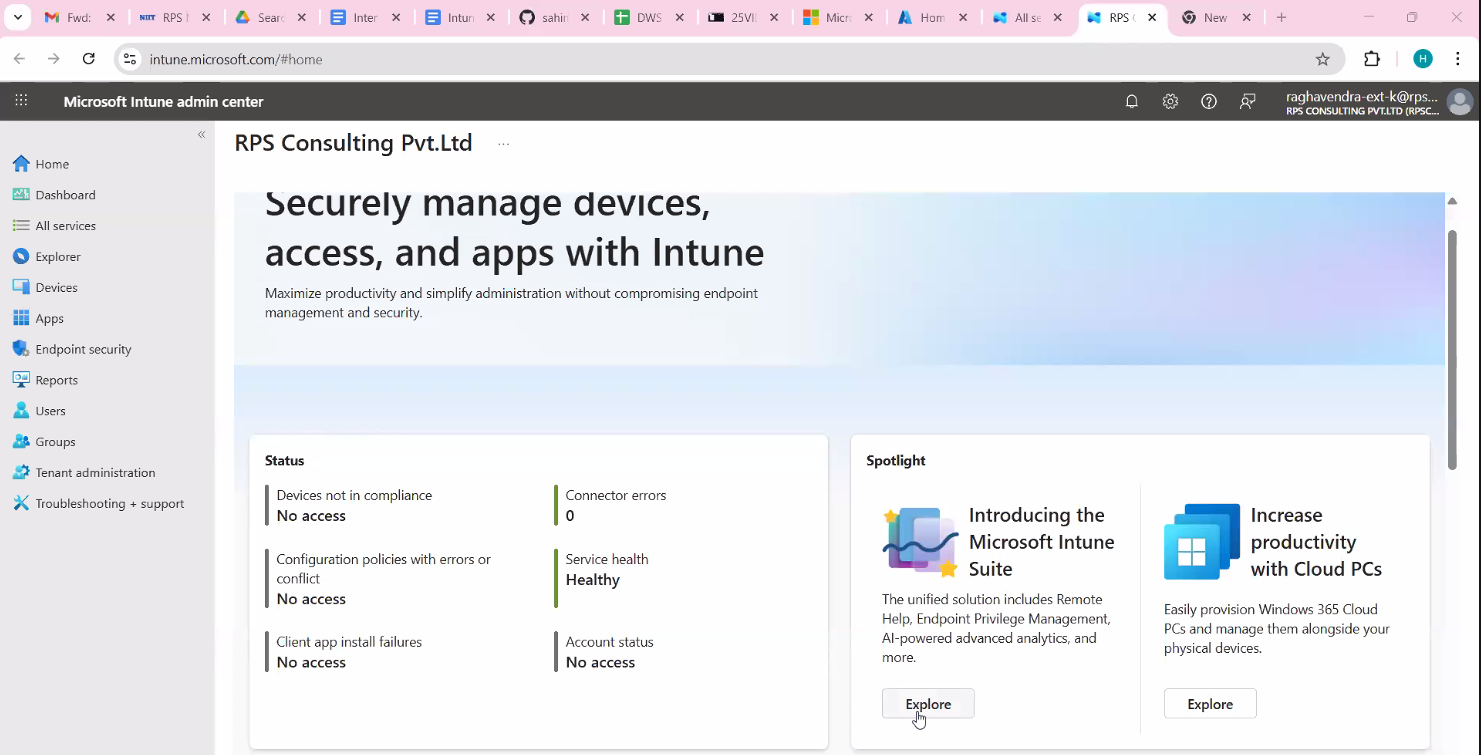
2. IME reports status to Intune: The IME service reports the installation status to Intune.

**Step 6: Toast Notifications**

1. Success notification: If the installation is successful, the IME service displays a toast notification to the user.

2. Failure notification: If the installation fails, the IME service displays a toast notification to the user with error details.





**LOB Apps:**

1. Registry detection: Intune uses registry keys to detect the presence and installation status of LOB apps.

2. Custom detection rules: Administrators can define custom detection rules using registry keys and values to determine if the app is installed.

**Win32 Apps:**

1. Registry-based detection: Intune can use registry keys and values to detect the presence and installation status of Win32 apps.

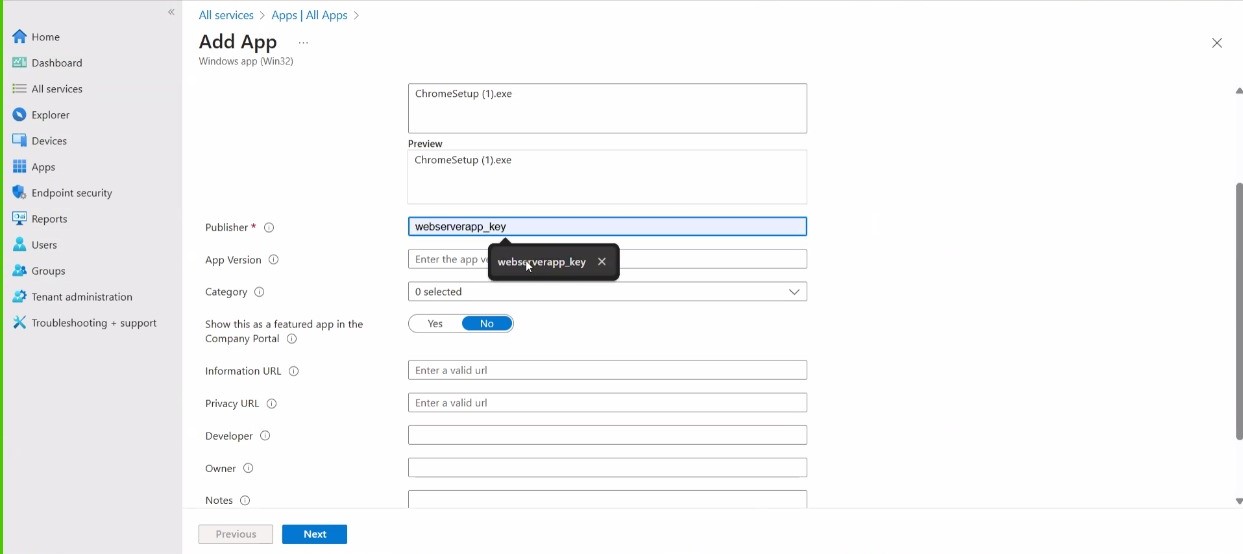
2. MSI and EXE installers: Win32 apps often use MSI or EXE installers, which can write registry keys during installation.

3. Custom install and detection scripts: Administrators can use custom scripts to install and detect Win32 apps, including registry-based detection.

**Registry Keys:**

1. HKLM (HKEY\_LOCAL\_MACHINE): Registry keys under HKLM are used for system-wide settings and detection.

2. HKCU (HKEY\_CURRENT\_USER): Registry keys under HKCU are used for user-specific settings and detection.



By leveraging registry keys and custom detection rules, administrators can effectively manage and detect LOB and Win32 applications in Intune.

**Application GUID:**

1. Each application has a unique GUID: The GUID is used to identify the application and track its installation status.

2. Registry key structure: The registry key for an application typically follows the format: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{GUID}

**Installation Status:**

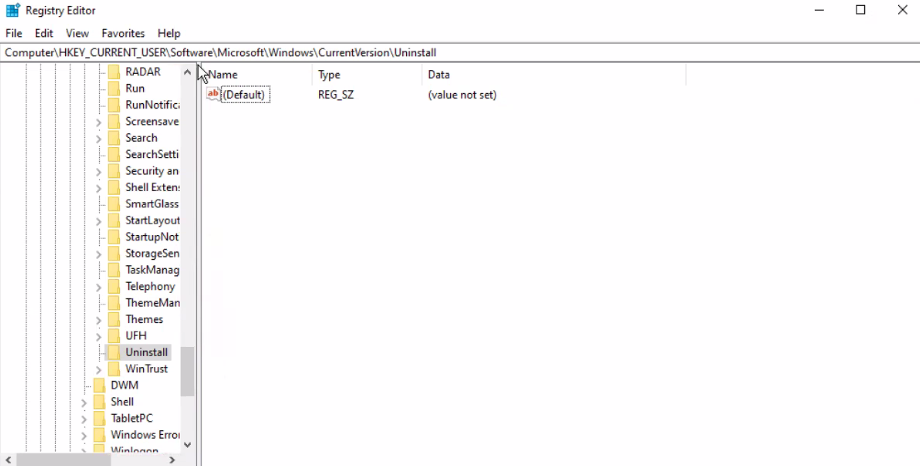
1. DisplayName: The display name of the application.

2. InstallDate: The date the application was installed.

3. UninstallString: The command line string used to uninstall the application.

**Uninstallation Status:**

1. When an application is uninstalled, its registry key may be removed or updated: The uninstallation status can be tracked by monitoring the registry key or using custom detection rules.



By querying these registry keys and using the Application GUID, you can determine the installation and uninstallation status of applications.

**Log File Locations:**

**Windows System Logs:**

1. Event Viewer: Windows Event Viewer logs system, security, and application events.

- Location: %SystemRoot%\System32\winevt\Logs

2. WindowsUpdate.log: Windows Update log file.

- Location (Windows 10/11): %SystemRoot%\Logs\WindowsUpdate

**Intune Logs:**

1. Intune Management Extension (IME) logs:

- Location: %ProgramData%\Microsoft\IntuneManagementExtension\Logs

2. IntuneWinAppUtil logs:

- Location: Varies depending on the execution location

**Application-Specific Logs:**

1. Custom log locations: Applications may store logs in custom locations, such as %ProgramData%\ApplicationName\Logs or %USERPROFILE%\AppData\Local\ApplicationName\Logs.

**Other Logs:**

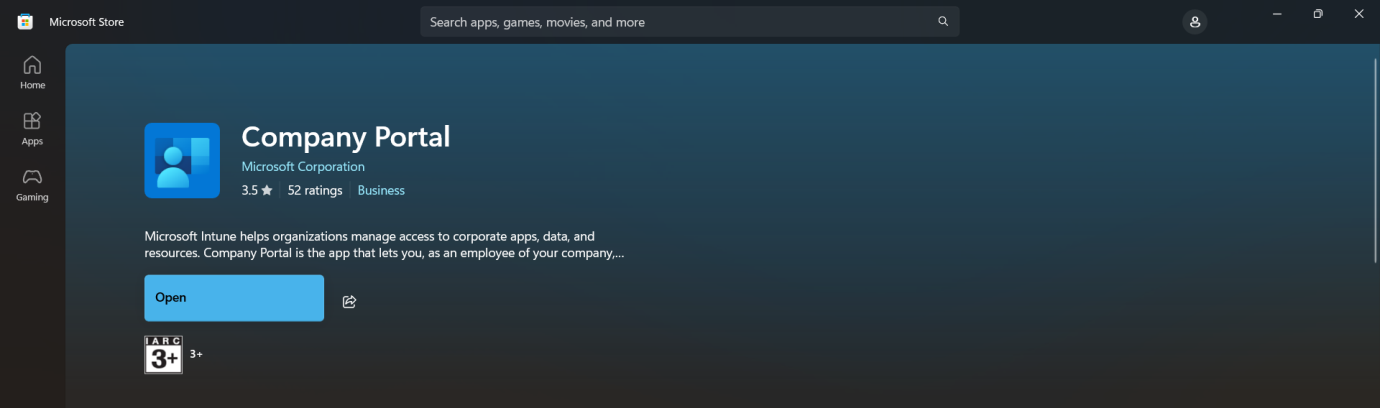
1. Setup and installation logs: %SystemRoot%\Logs\Setup

2. Windows Installer logs: %TEMP%\MSI\*.log

These log file locations can help you troubleshoot issues, monitor system activity, or analyze application behavior.

**Company Portal:**

Company Portal is a mobile app developed by Microsoft that enables employees to access company resources, apps, and data securely.



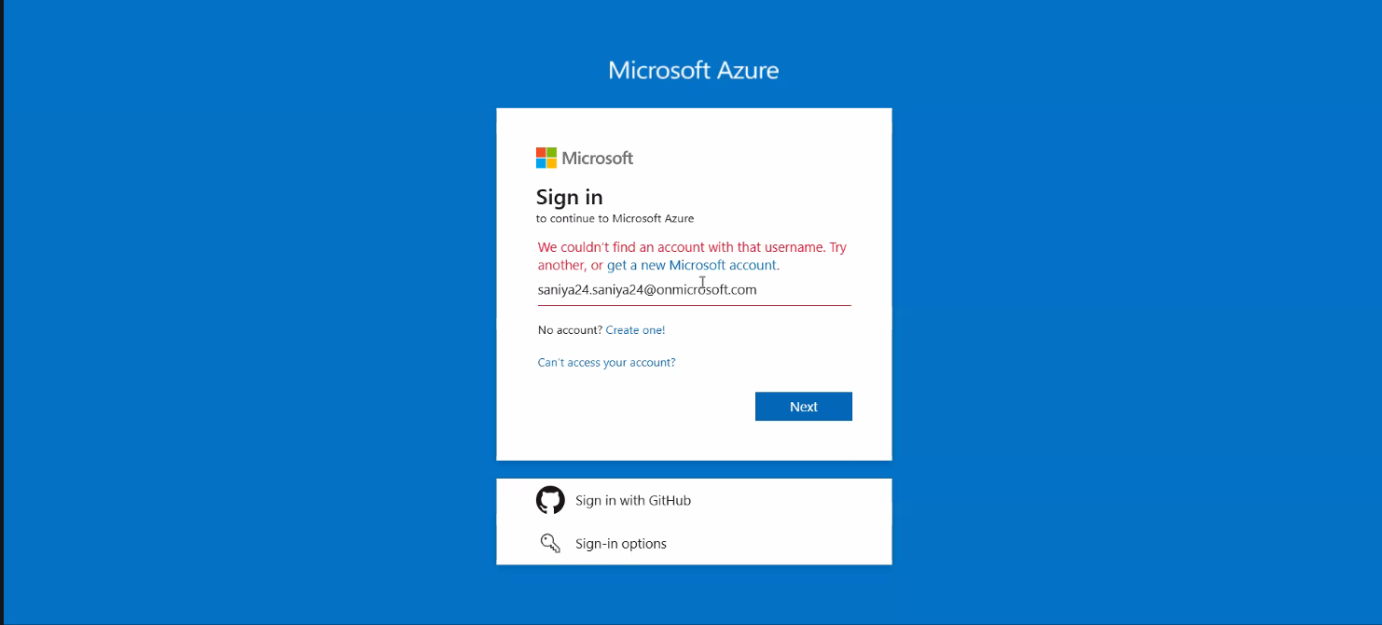
**How to sync once app assignments are done:**

**Intune Portal (Azure Portal):**

1. Navigate to the Microsoft Endpoint Manager admin center: [(link unavailable)]((link unavailable))

2. Go to Devices: Select the device group or individual device you want to sync.

3. Sync: Click on the "Sync" button to initiate a sync.



**Company Portal App (Device-Side):**

1. Open the Company Portal app: On the device, open the Company Portal app.

2. Settings: Tap on the menu (three horizontal lines or dots) and select "Settings."

3. Sync: Tap on "Sync" to initiate a local sync.

**Device-Side Sync (Additional Methods):**

1. Pull down to refresh: In the Company Portal app, pull down on the device list to refresh and sync.

2. Check-in: Some devices may require a manual check-in to sync with Intune.

**When to Sync:**

1. After assigning apps or policies: Sync devices after assigning new apps or policies to ensure they receive the updates.

2. When troubleshooting: Sync devices when troubleshooting issues to ensure the latest policies and apps are applied.

**Log File Events:**

1. Info: Informational messages, such as:

- Application startup or shutdown

- User login or logout

- Policy application or updates

2. Warning: Warning messages, such as:

- Potential issues or unexpected events

- Configuration conflicts or overrides

3. Error: Error messages, such as:

- Application crashes or failures

- Policy application failures

- Connectivity issues

4. Verbose: Detailed, step-by-step information, often used for:

- Troubleshooting complex issues

- Debugging application behaviour

**Log File Structure:**

1. Timestamp: Date and time of the event

2. Event ID: Unique identifier for the event

3. Component: Module or component generating the event

4. Message: Description of the event

**Common Log File Analysis Tasks:**

1. Filtering: Filtering events by type (e.g., errors, warnings)

2. Searching: Searching for specific keywords or event IDs

3. Correlating: Correlating events across multiple log files or systems

**By analyzing log files, you can:**

1. Troubleshoot issues: Identify root causes of problems

2. Monitor system health: Detect potential issues before they become critical

3. Optimize performance: Identify areas for improvement