# Batch Information:

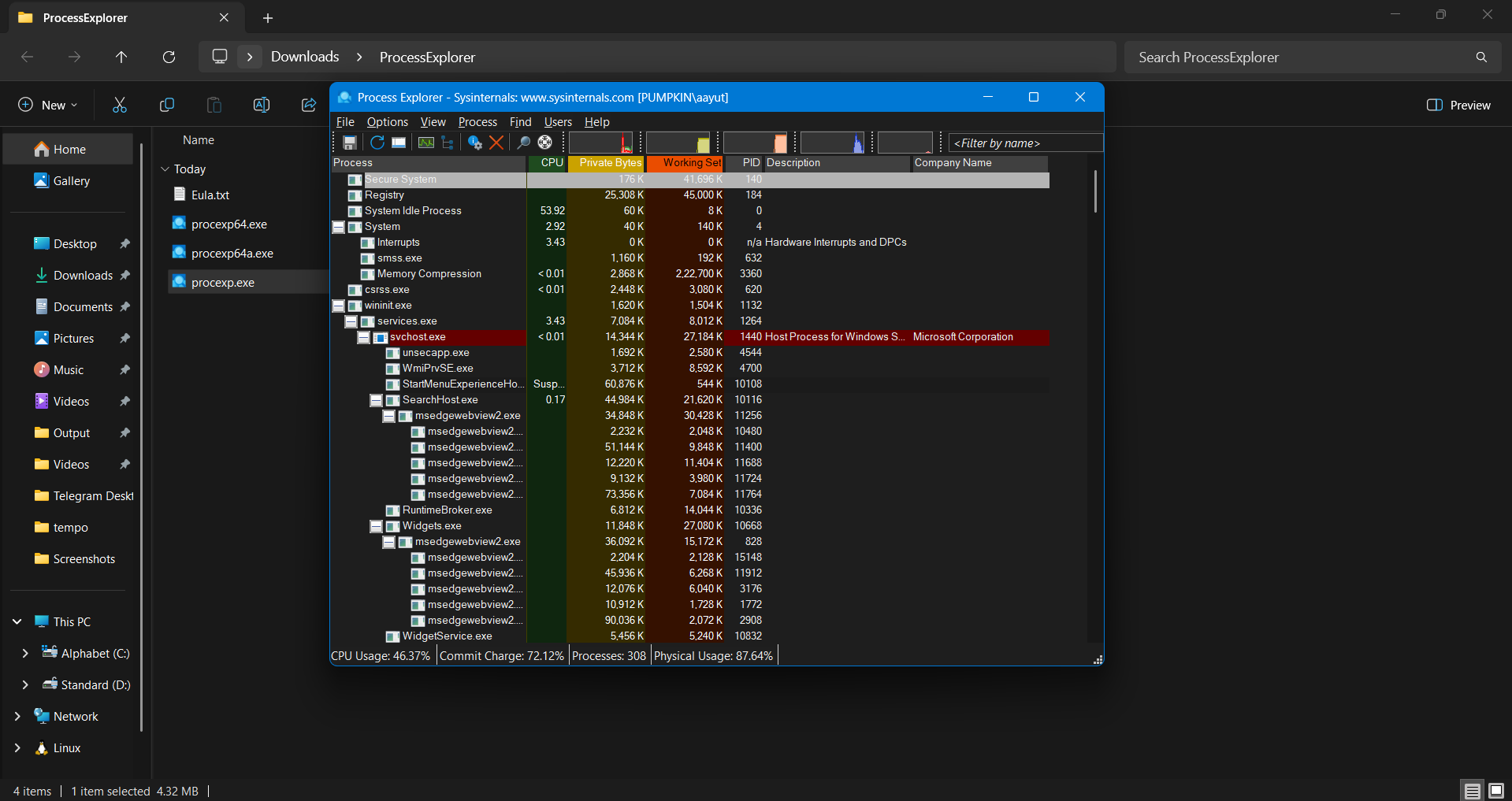
* **Batch Start Date:** 2025-08-04
* **Batch Name:** WiproNGA\_DWS\_B5\_25VID2550
* **First Name:** Aayush
* **Last Name:** Kumar
* **User ID:** 34758
* **Batch ID:** 25VID2550

**Assignment**

**Windows Debugging Tools**

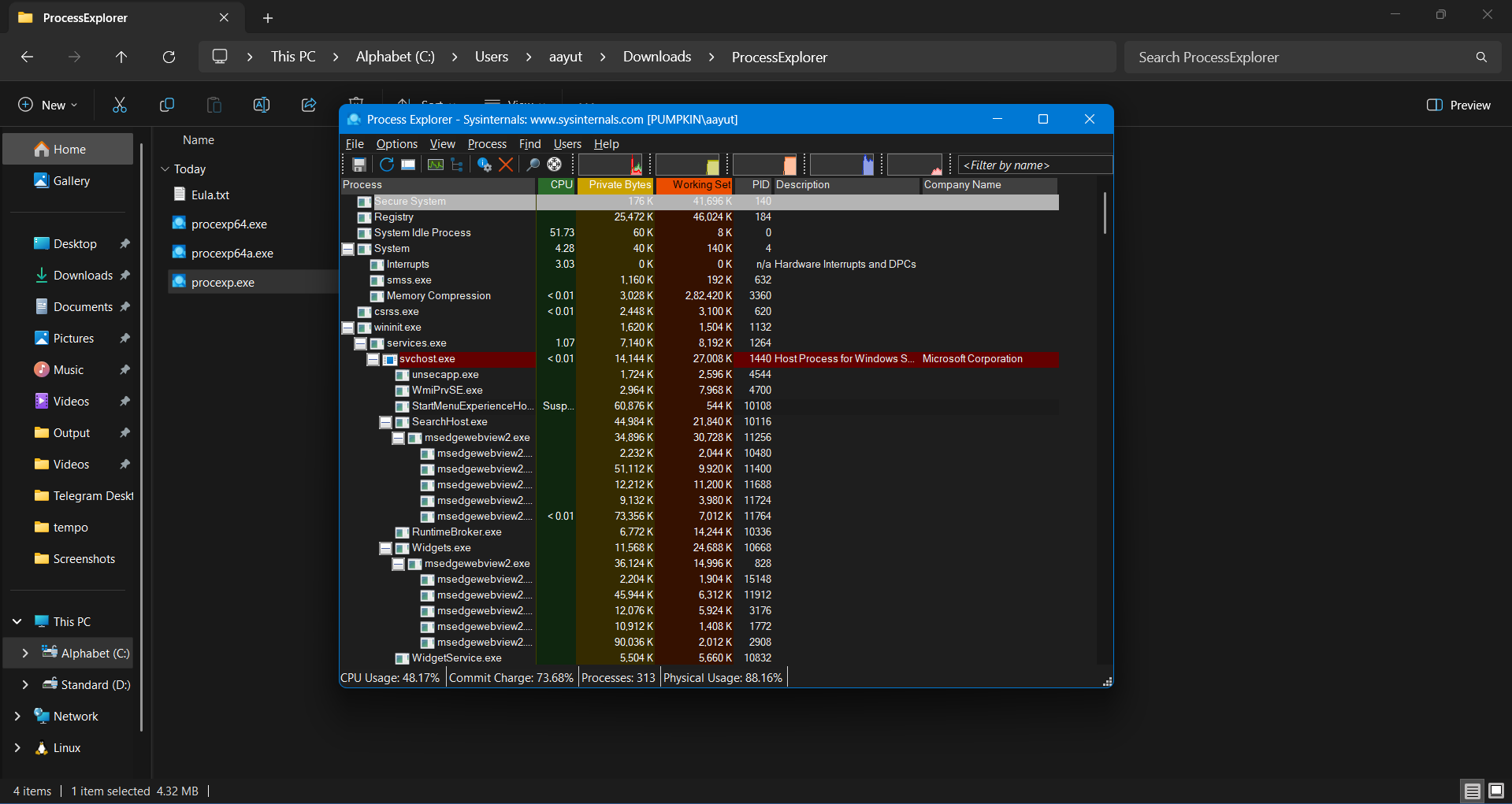
**Process Explorer:-**

This utility serves as a highly sophisticated and essential system monitoring and management tool, enabling users to view, analyze, and control all active processes running on a computer in real time. It provides comprehensive and granular information, including CPU and memory consumption, thread activity, open file handles, loaded modules, network usage, and file dependencies associated with each process. By presenting such in-depth insights, it empowers system administrators, developers, and advanced users to pinpoint performance bottlenecks, diagnose software malfunctions, and resolve system slowdowns with precision. Furthermore, it plays a crucial role in security monitoring, enabling the detection of hidden or suspicious background activities such as unauthorized processes, malware, or resource hijacking. In essence, it acts as both a diagnostic instrument and a defense mechanism, offering deep visibility into the operating system’s internal workings.



**Process Monitor**

Process Monitor is an advanced Windows diagnostic utility designed to capture and analyze the real-time interactions between processes, the file system, and the registry. It offers granular visibility into system operations by logging every system call and event related to process execution, including memory allocation patterns, thread creation/destruction, access to files and directories, registry reads/writes, and modifications to system objects. Through its detailed event tracing, Process Monitor exposes the full lifecycle of processes, revealing information such as inherited handles, module loading, inter-process communication, and network activity.

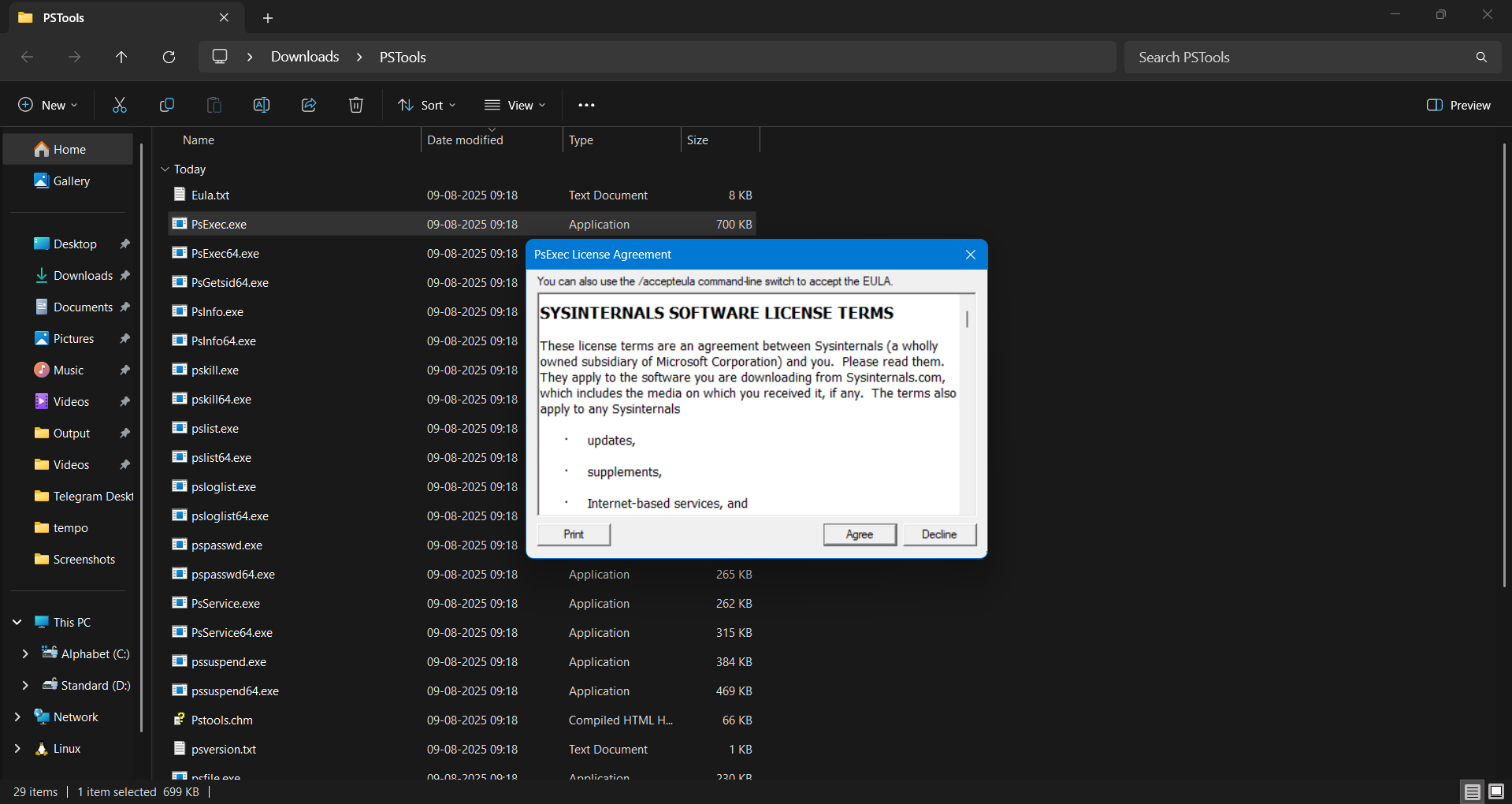


**PS tools**

PsTools (Process Status Tools) is a comprehensive suite of command-line utilities developed by Sysinternals, tailored for system administration and troubleshooting within Windows environments. This toolkit includes a variety of specialized tools such as PsExec, PsLoggedOn, PsKill, PsFile, PsList, among others, each serving distinct administrative purposes.

PsExec allows administrators to execute programs remotely without requiring remote desktop access, facilitating remote management and automation. PsLoggedOn reveals users currently logged onto a system, while PsKill enables terminating processes by name or process ID. PsFile tracks files opened remotely on the system, and PsList provides detailed information about running processes, including CPU and memory usage.

Together, these utilities empower IT professionals to efficiently manage both local and networked Windows systems by viewing active users, monitoring and controlling processes, handling opened files, and executing commands remotely. This extensive functionality makes PsTools an essential toolkit for advanced system administration, troubleshooting, and automation in enterprise environments. It is especially valuable for IT administrators who require powerful, scriptable, and remote management capabilities without the overhead of graphical interfaces.

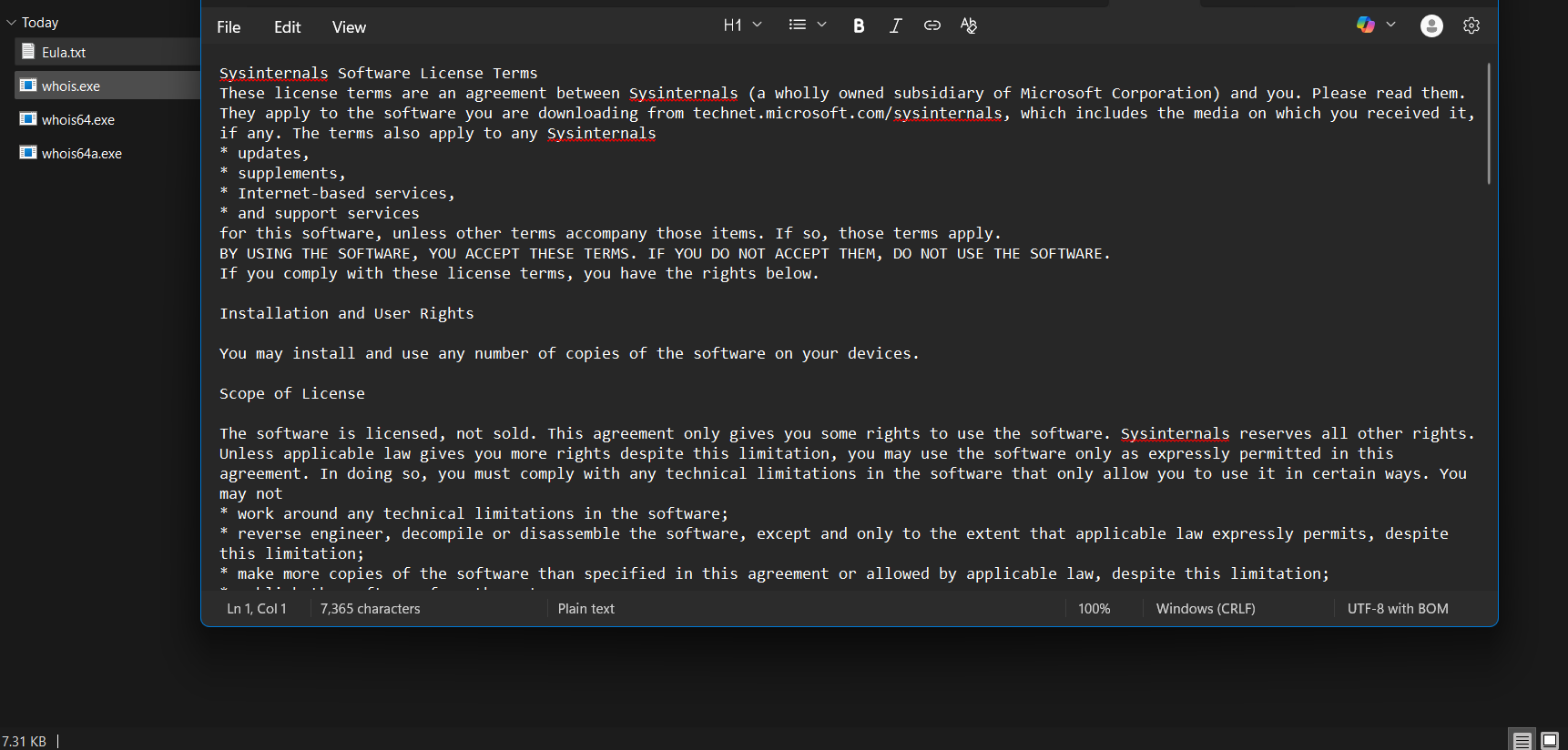


**Whois**

Whois is a command-line utility widely used for obtaining comprehensive information about domain names and IP addresses by querying publicly accessible Whois databases. While not originally part of the Sysinternals suite, it is commonly included in many system and network administration toolkits due to its valuable functionality.

The Whois tool retrieves key domain registration details such as the registrant's name, contact information, registration and expiration dates, domain status, and the relevant registrar organization. This information is crucial for verifying domain ownership and administrative contacts, which helps in network troubleshooting, cybersecurity investigations, and monitoring domain name status.

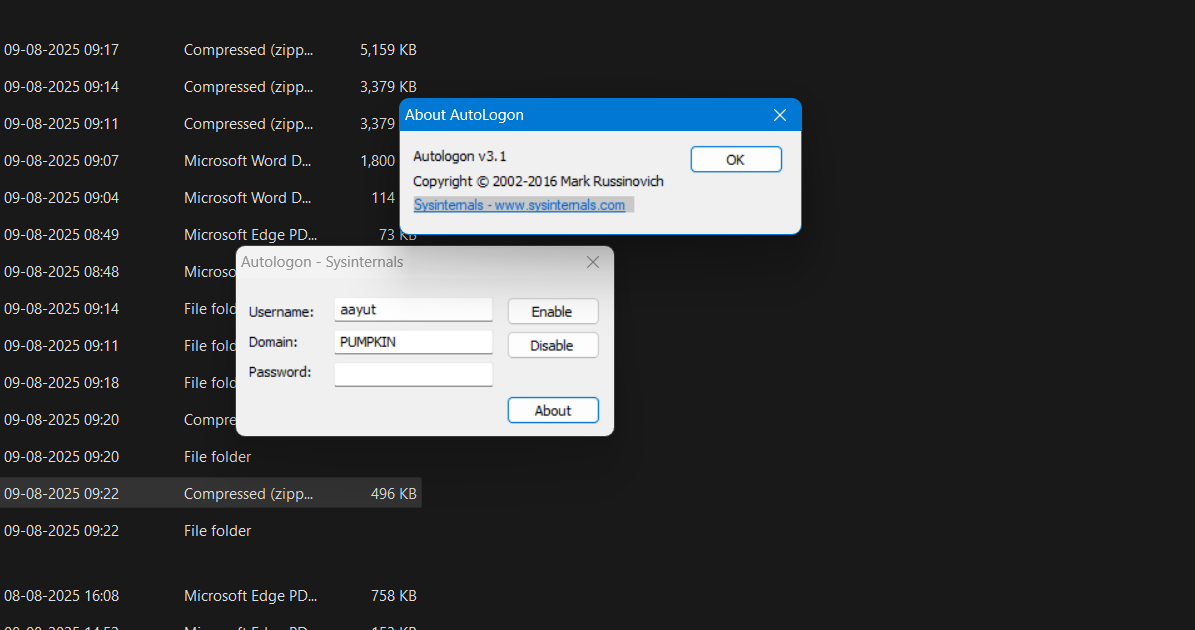
In practical use, Whois aids IT professionals and network administrators by enabling them to track down the source of malicious or suspicious online activity, validate domain legitimacy, and assess domain availability before registration. Its role in enhancing transparency on the internet makes it an essential command-line utility for managing and investigating domain-related issues in both small-scale and enterprise environments.



**Autologon**

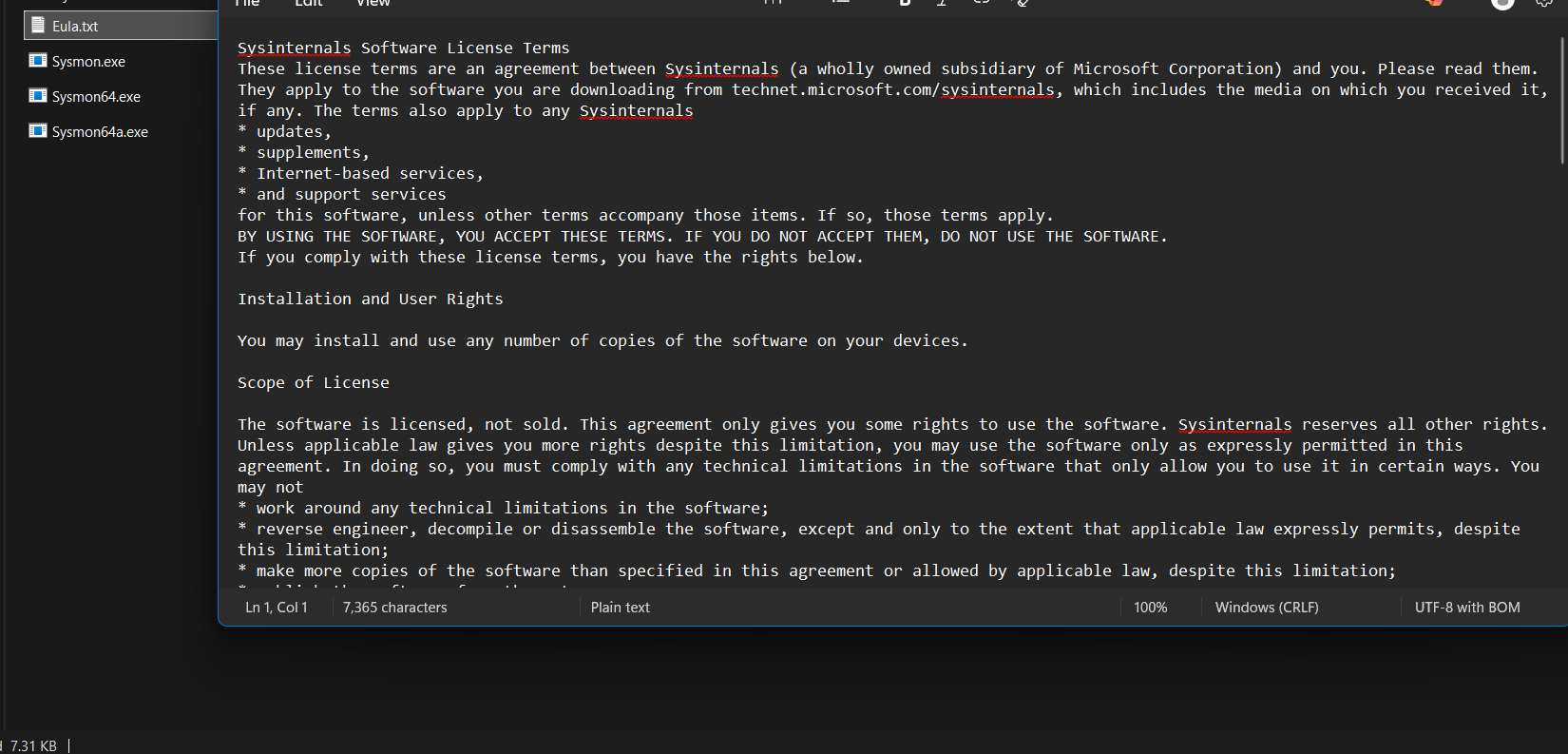
A graphical utility designed to automate the Windows login process. It securely stores user credentials—username and password—in the Windows registry in an encrypted form. Once configured, Autologon allows a specified user account to log in automatically during system startup without requiring manual credential entry.

This tool is especially useful in scenarios such as headless systems, kiosks, or automated testing environments where manual login would be impractical or disruptive. Autologon fundamentally enables Windows’ built-in auto-login feature by making the necessary registry changes to store the credentials as *LSA secrets*. Although the credentials are encrypted, users with administrative privileges can potentially retrieve and decrypt them, so it should be used with caution in secure environments.



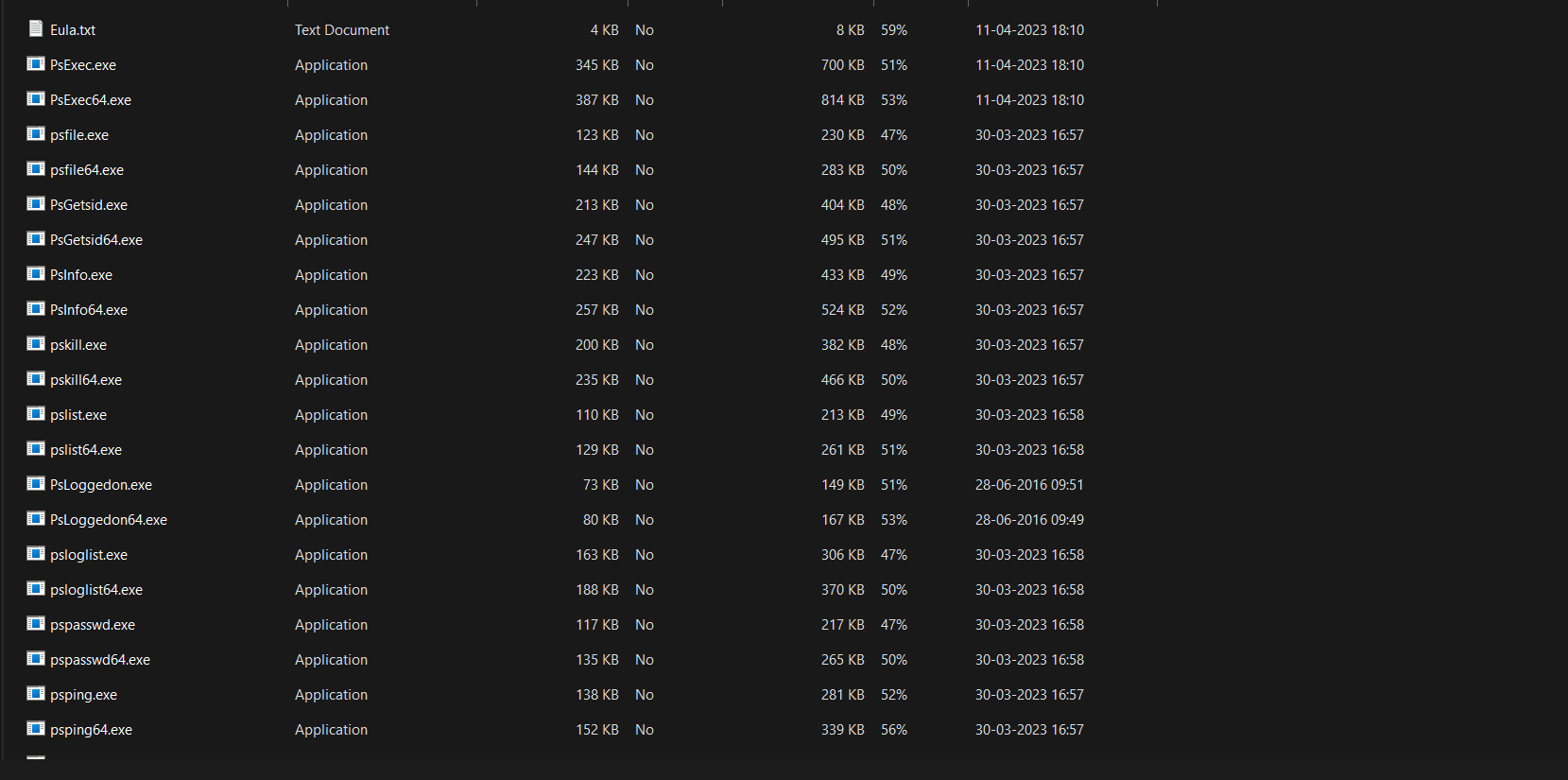
**Sysmon (System Monitor)**

Sysmon, short for System Monitor, is a Windows system service and device driver developed by Microsoft as part of the Sysinternals suite. Once installed, it runs continuously across system reboots to provide detailed and advanced logging of system activity directly to the Windows Event Log. Sysmon captures rich event data including process creations with full command lines, network connections (with source and destination IPs and ports), changes to file creation timestamps, image loadings, and more.



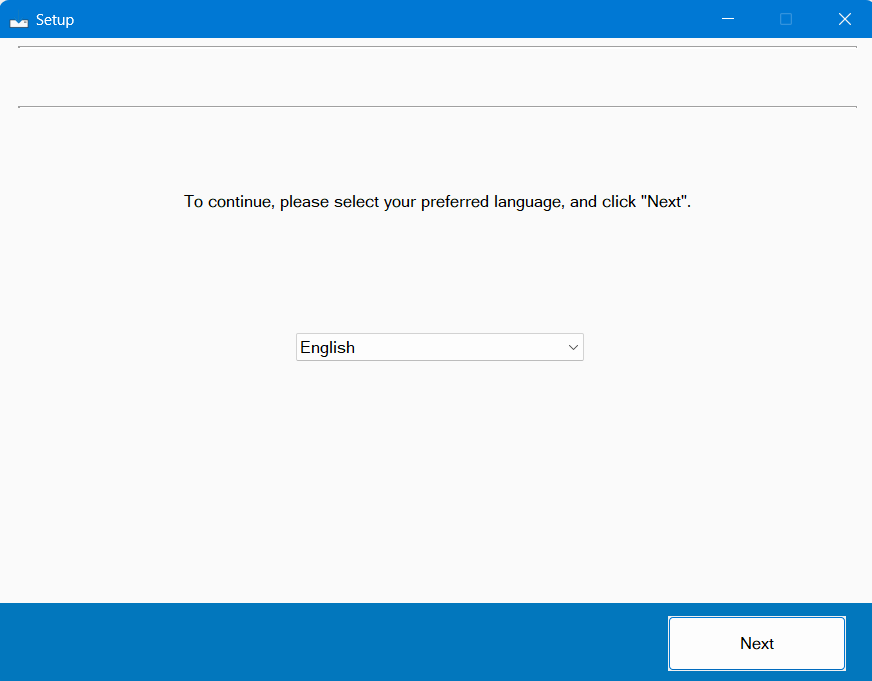
**PsExec**

PsExec is a versatile command-line utility within Microsoft’s Sysinternals PsTools suite, designed to execute processes on remote Windows systems with the same authority and behavior as if they were run locally. It operates without requiring Remote Desktop Protocol (RDP) sessions or manual physical access, instead leveraging built-in Windows networking protocols (notably SMB and the Service Control Manager) to transfer and initiate executables on target machines.

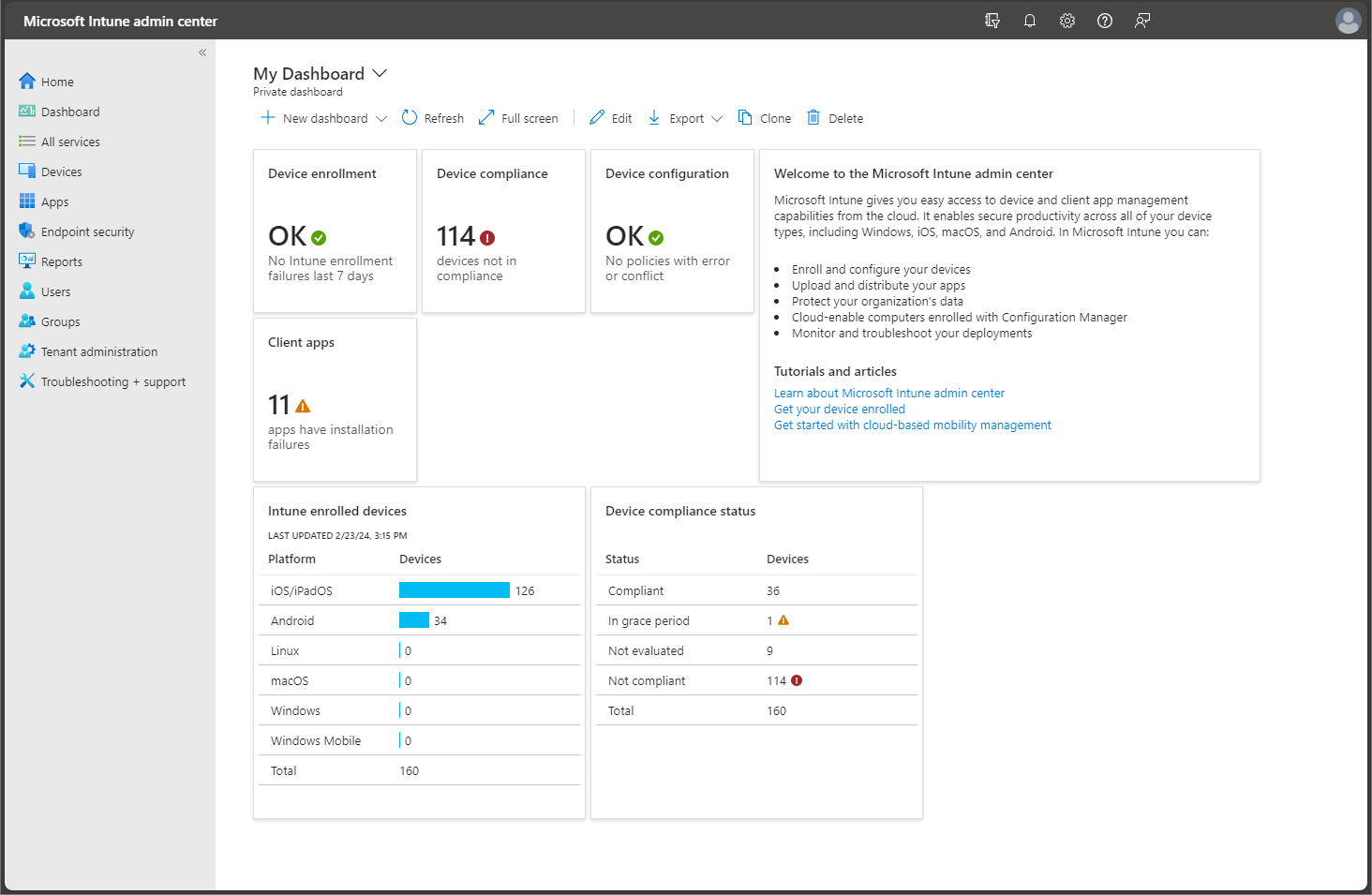


**RegMon**

RegMon is a Windows-based real-time registry monitoring tool that logs and displays all registry activities happening on the system. It records every read, write, and delete operation, along with details about the process responsible for the action and the specific keys or values accessed or modified. This tool is particularly valuable for troubleshooting registry issues, detecting unauthorized or suspicious programs that alter the registry, and analyzing potential security risks or system vulnerabilities.



**Microsoft Inture portal Steps**



1. **Sign In**
   * **Go to**[**https://intune.microsoft.com**](https://intune.microsoft.com/)**and sign in using a Global Admin account.**
2. **Assign Intune License**
   * **In the Microsoft 365 Admin Center, navigate to Users.**
   * **Assign Intune licenses to the users who need device management.**
3. **Set MDM Authority**
   * **In the Intune Admin Center, go to Tenant Administration.**
   * **Set Microsoft Intune as the Mobile Device Management (MDM) authority.**
4. **Enroll Devices**
   * **Navigate to Devices → Enroll Devices.**
   * **Set up platform-specific enrollments for Windows, Android, and iOS devices.**
5. **Create Policies**
   * **Compliance Policy: Define rules such as password requirements and minimum OS versions.**
   * **Configuration Profile: Configure settings like Wi-Fi, security options, and Microsoft Defender settings.**
6. **Add Applications**
   * **Go to Apps → All Apps → Add.**
   * **Upload or select applications to deploy and assign them to users or devices.**
7. **Monitor**
   * **Use the Monitor section to track the health of devices, app deployment status, and compliance with your policies.**