# Batch Information:

* Batch Start Date: 2025-08-06
* Batch Name: WiproNGA\_DWS\_B7\_25VID2557
* First Name: B S Shrawani
* User ID: 34932
* Batch ID: 25VID2557

ASSIGNMENT

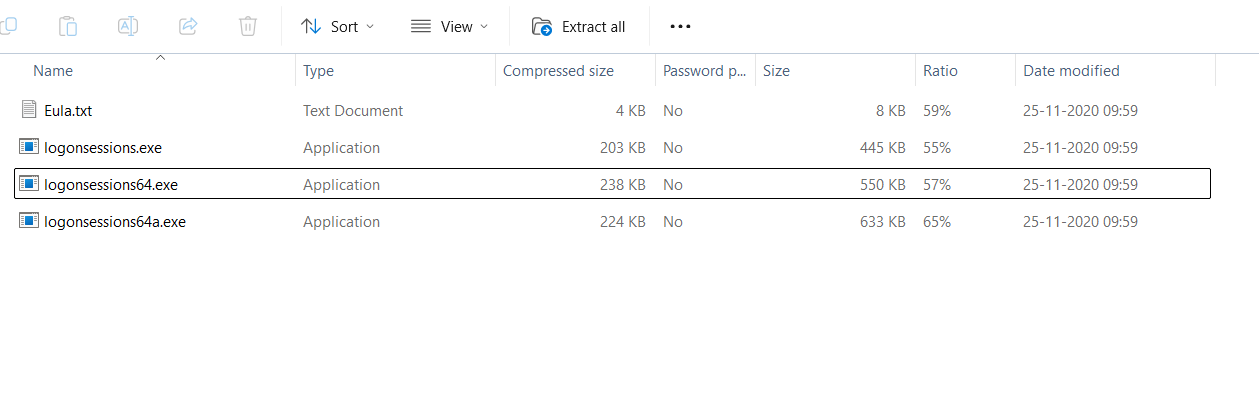
***Topics-Using Windows Tools for Debugging: LogonSessions, Autologon, Process Explorer, Psexec, PSTools, RegMon, Whois, SysMon. Intune Free trial Subscription - How to enrol.***

Introduction : Windows provides a comprehensive set of tools for debugging, ranging from user-mode application debugging to kernel-mode driver and system service debugging. The primary tools are part of the Debugging Tools for Windows package, which can be obtained as part of the Windows SDK or the Windows Driver Kit (WDK).

In Windows environments, especially in enterprise IT and system administration tasks like Application Packaging, System Monitoring, and Debugging, Microsoft and Sysinternals provide a set of powerful utilities. These tools help investigate performance issues, identify unauthorized access, understand registry behavior, and automate system tasks.

## LogonSessions

* + **Purpose**: Displays all user logon sessions on the system.
  + **Tool**: Part of Sysinternals Suite (command-line tool: LogonSessions.exe)
  + **Use Case:**
    - Identifying active user sessions.
    - Detecting suspicious logon activity.



## Autologon

* + **Purpose**: Enables automatic login to Windows without entering a password at startup.
  + **Tool Type**: GUI tool from Sysinternals.
  + **Use Case:**
    - Useful for kiosks, test environments, or VM automation where secure unattended logon is needed.
  + **How it works:**
    - It stores credentials securely in the registry:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

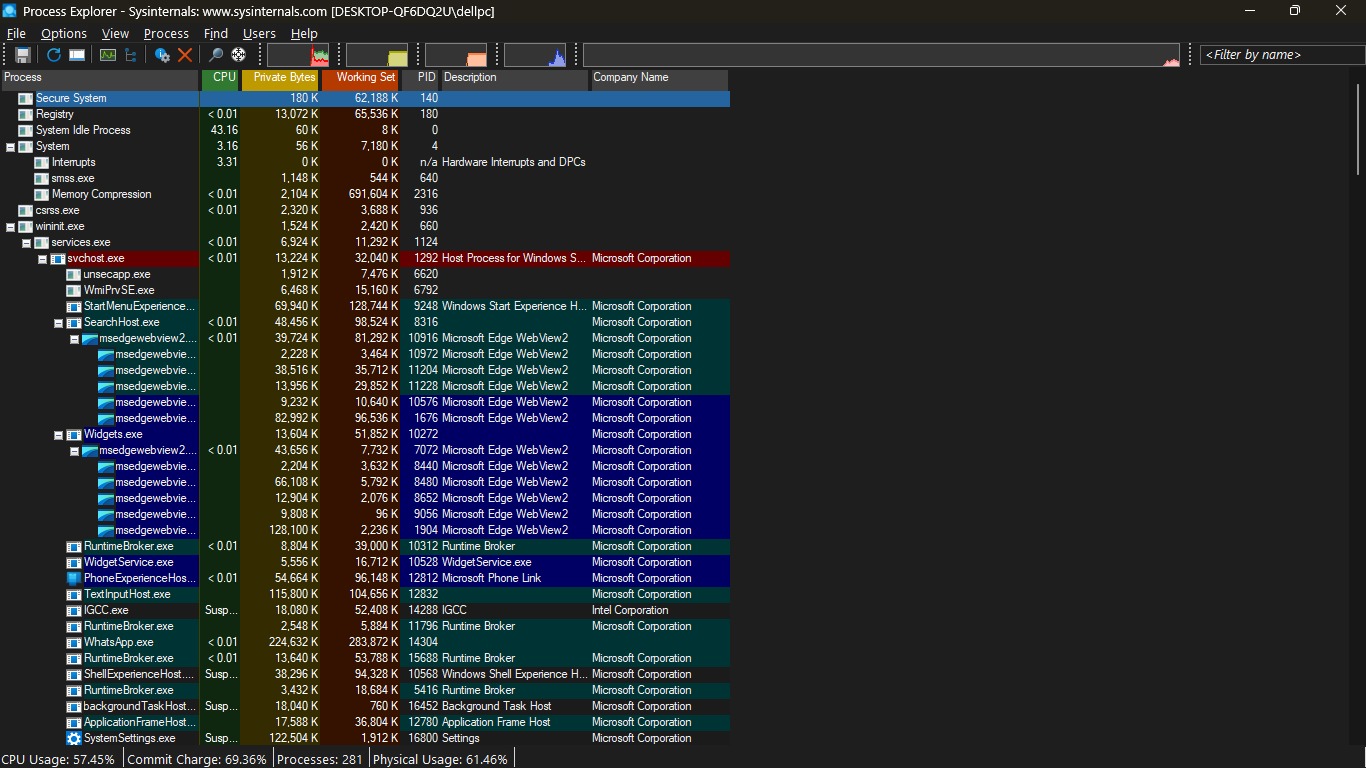
* + **Important**: Autologon encrypts the password and hides it from plain view.

## Process Explorer

* + **Purpose**: Advanced version of Task Manager with detailed insight into system processes.
  + **Tool Type**: GUI

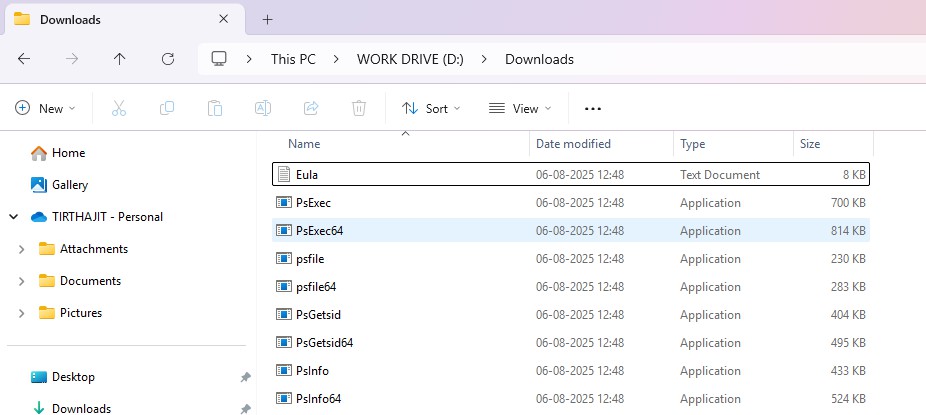
## Use Case:

* + - Analyze running processes.
    - Detect malware or injected DLLs.
    - Check parent-child process trees.
    - Monitor file, registry, and DLL activity per process.



## PsExec

* + **Purpose**: Execute processes on remote systems.
  + **Tool Type**: Command-line tool in **PsTools suite**
  + **Use Case:**
    - Remotely launch applications
    - Run command-line tools on other machines without RDP.



## PsTools Suite (Collection)

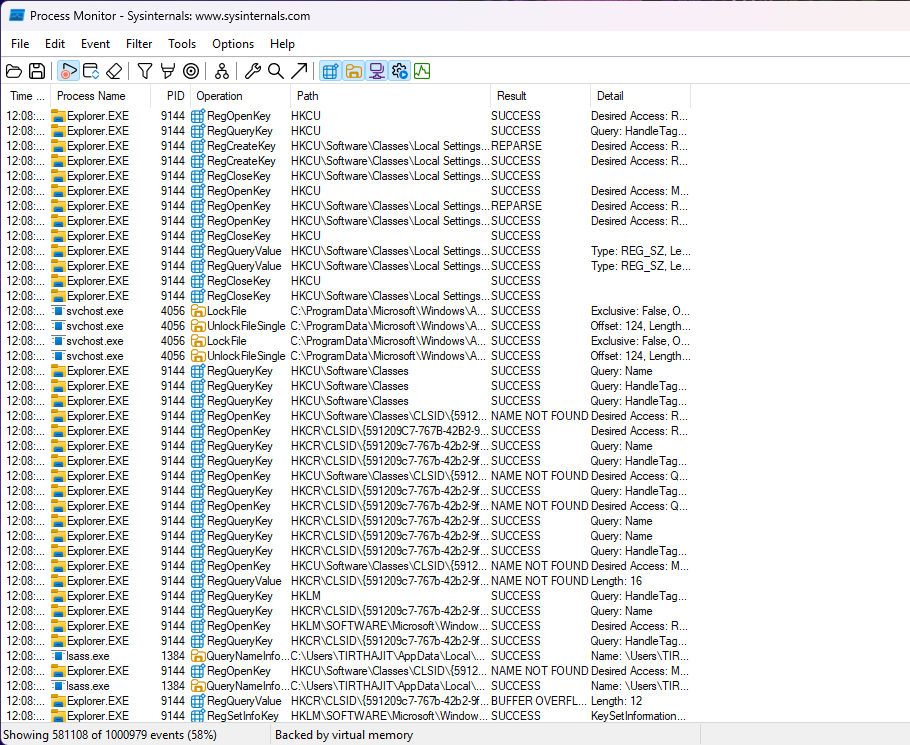
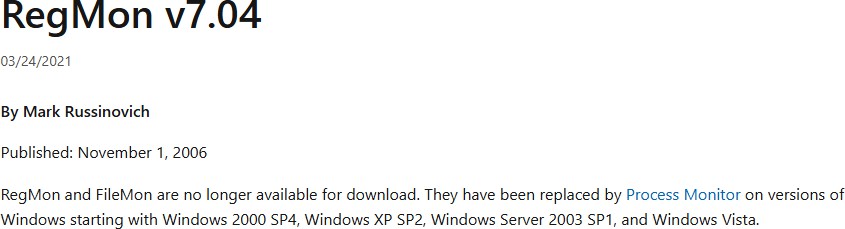
* + A suite of **remote administration tools** for managing local and remote systems.
  + Tools include:
    - PsExec – Run remote commands
    - PsList – Show process list
    - PsKill – Kill processes
    - PsLogList – Event log viewer
    - PsShutdown – Remotely shutdown/reboot
    - PsService – Control services
  + **Use** **Case**:
    - Great for scripting administrative tasks across multiple systems.

1. **RegMon *(Note: Replaced by Process Monitor)***
   * **Purpose**: Real-time monitoring of Registry access.
   * **Status**: Now merged into **Process Monitor**.
   * **Use Case:**
     + Debug registry reads/writes during software installs.
     + Identify which keys are modified by applications.

## 

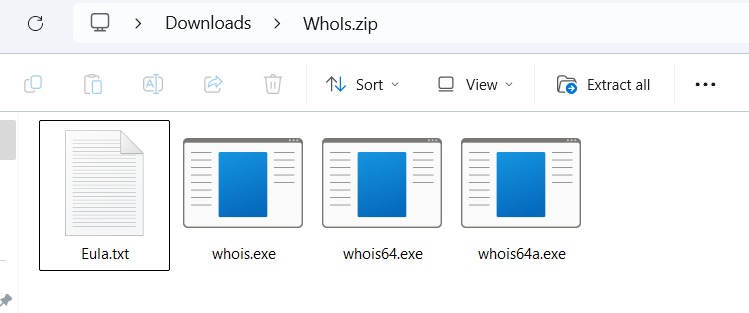
EXAMPLE

* + - Monitor what registry keys an installer touches during execution.
  + **Replaced by**: Use ProcMon instead, with filters for Operation = RegSetValue, etc.



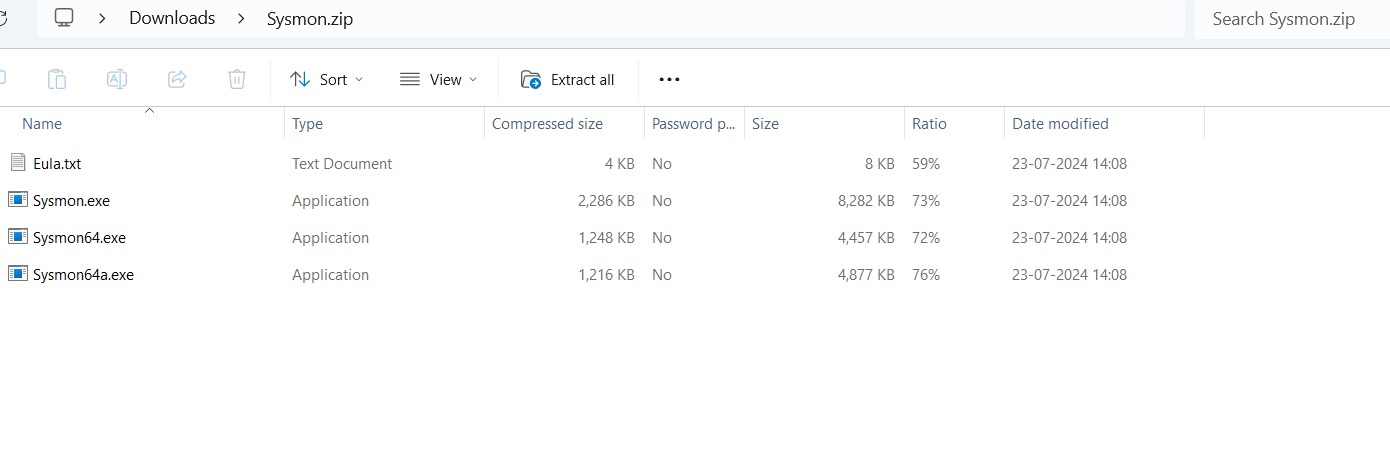
## Who is

* + **Purpose**: Query domain registration details.
  + **Tool Type**: Command-line tool.
  + **Use Case:**
    - Troubleshooting suspicious network connections or domains,
    - Identifying the owner of a domain or IP.



## Sysmon (System Monitor)

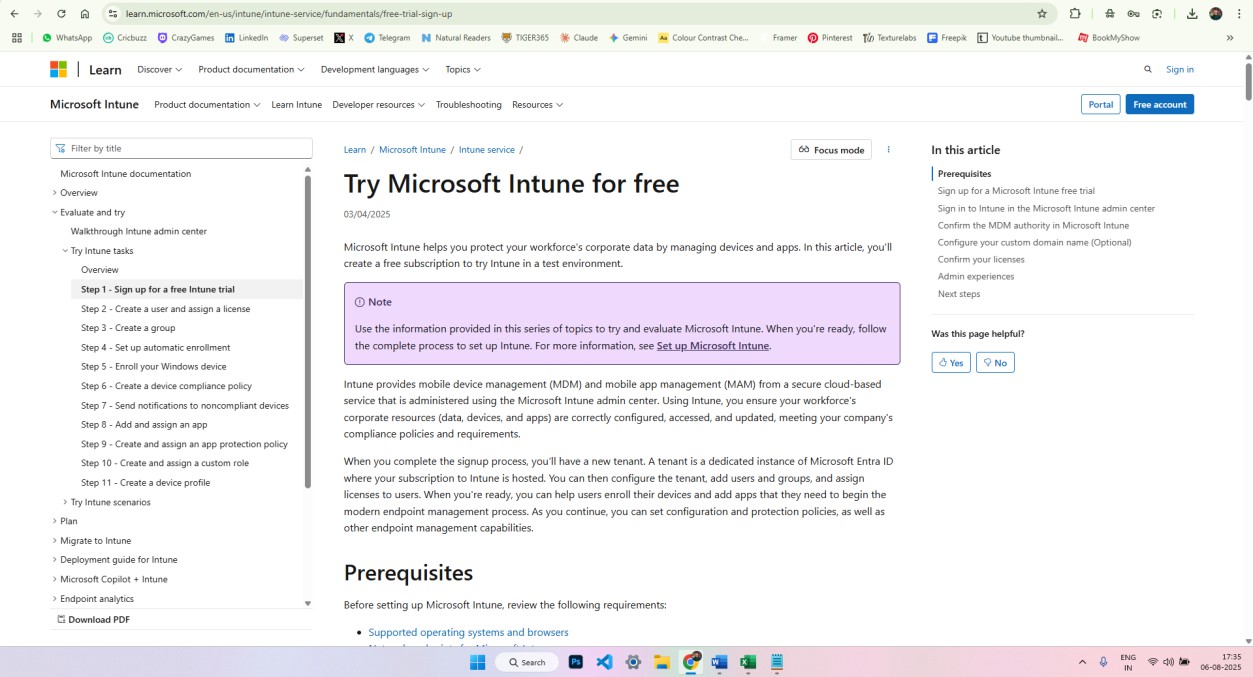
* + **Purpose**: Logs detailed system activity to the Windows Event Log.
  + **Tool Type**: Service + Driver
  + **Use Case:**
    - Monitor:
      * Process creation
      * Network connections
      * File creation time changes
      * Registry modifications
    - Used in security analytics and threat detection.



# Intune Free trial Subscription - How to enrol

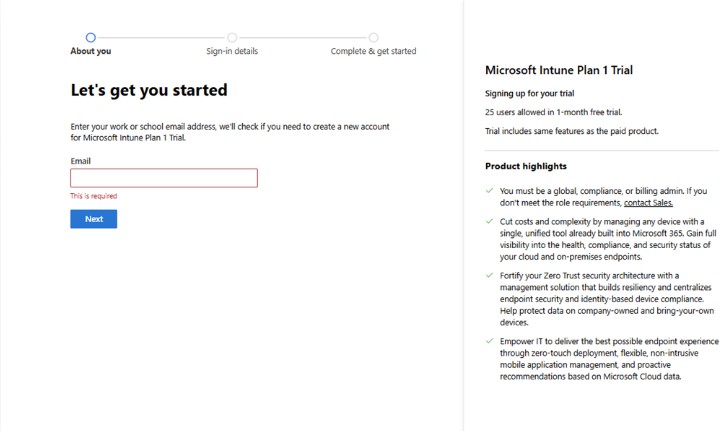
## Access the Intune Setup Account Page:

* + Open a web browser and go to the Intune setup account page.



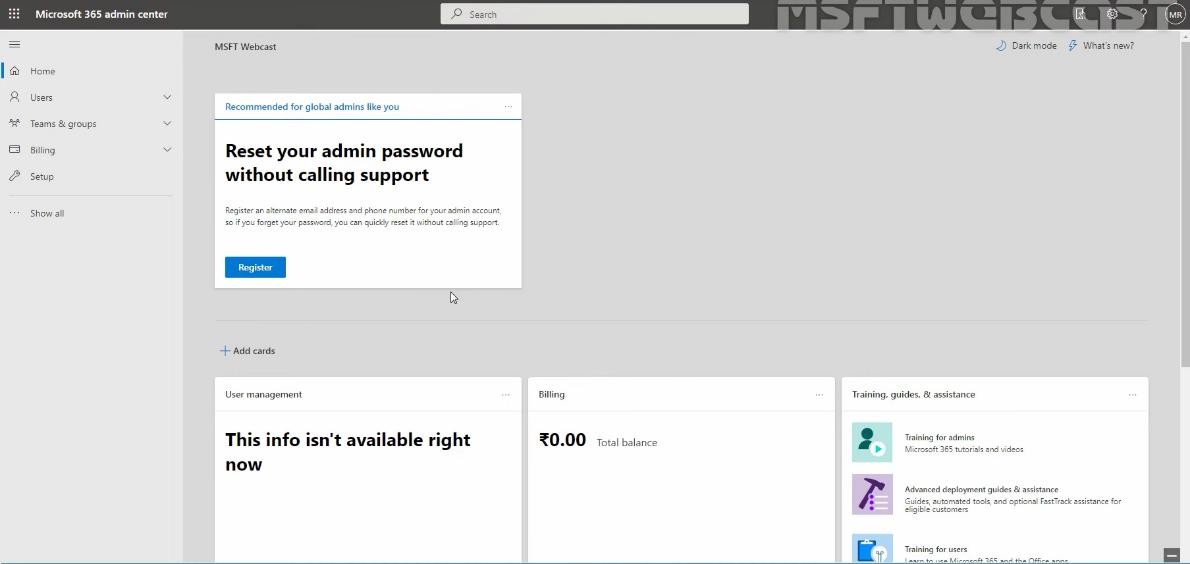
## Sign Up or Sign In:

* + **For new users:** Enter your email address and click "Next." Follow the prompts to create a new account and provide the necessary information.
  + **For existing users:** Sign in with your existing work or school account.



## Complete the Sign-Up Process:

* + If creating a new account, you'll be asked to verify your email address and potentially provide additional information like your name, company details, and region.
  + After signing up or signing in, you'll be directed to the Microsoft 365 Admin Center.



## Considerations for Existing Work or School Accounts:

* + If you're using an existing work or school account, you might need to add Intune to your existing subscription.
  + If you plan to use your organization's custom domain name or synchronize with on- premises Active Directory, you might need to close the browser window after the initial setup and configure these aspects separately.

## Accessing Intune After Enrollment:

* + Once the free trial is set up, you can access the Microsoft Intune Admin Center to manage the service.
  + You can use any device with a supported browser to sign in.

