

**Batch Information:**

- **Batch Start Date:** 2025-08-04
- **Batch Name:** WiproNGA\_DWS\_B5\_25VID2550
- **First Name:** Kamran
- **Last Name:** Akmal
- **User ID:** 34958
- **Batch ID:** 25VID2557

# Assignments

## Topics

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

### Introduction

In Windows environments, troubleshooting application issues, installations, and security events often requires specialized utilities. The Sysinternals suite and other Windows tools provide deep insights into processes, registry activity, network connections, and system behavior. This assignment explains key tools including LogonSessions, Autologon, Process Explorer, PsExec, PsTools, RegMon, Whois, and Sysmon, along with their functionalities and use cases in debugging.

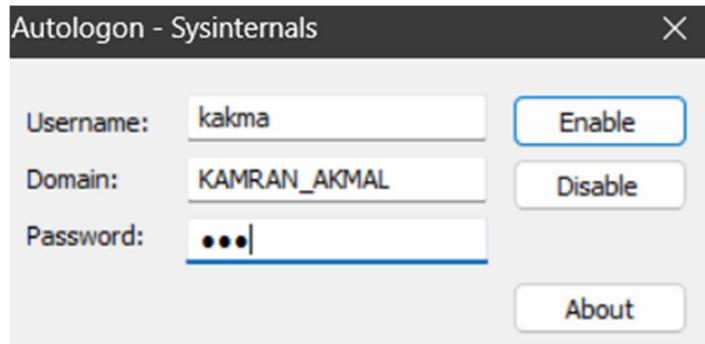
#### 1. LogonSessions

- **Purpose:** Displays information about all active logon sessions on a computer.
- **Key Details:**
  - Shows logon session IDs, usernames, logon type (interactive, service, remote), and authentication method.
  - Useful for auditing current and past user sessions.
- **Use in Debugging:**
  - Detects orphaned sessions that might lock resources.
  - Helps trace suspicious logins during incident response.

Name	Date modified	Type	Size
Eula.txt	06-08-2025 12:09 PM	Text Document	8 KB
logonsessions.exe	06-08-2025 12:09 PM	Application	445 KB
logonsessions64.exe	06-08-2025 12:09 PM	Application	550 KB
logonsessions64a.exe	06-08-2025 12:09 PM	Application	633 KB

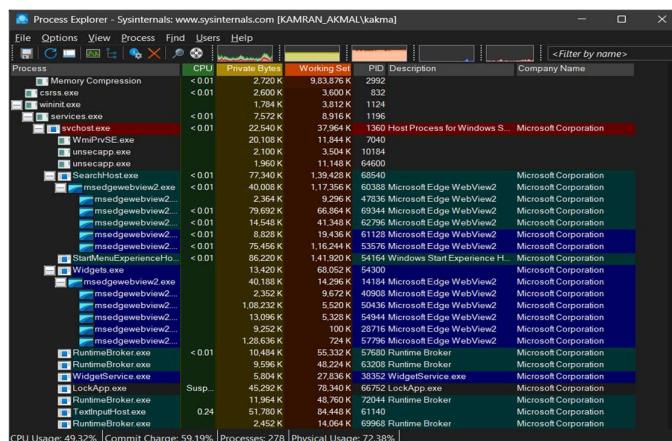
## 2. Autologon

- **Purpose:** Configures Windows to automatically log in with specified credentials.
- **Key Details:**
  - Credentials are encrypted in the registry and used during system startup.
  - Removes the need for manual user input at every reboot.
- **Use in Debugging:**
  - Automates repeated testing cycles after system reboots in packaging environments.
  - Speeds up virtual machine testing scenarios where manual logon delays progress.



## 3. Process Explorer

- **Purpose:** Advanced process management tool, often referred to as “Task Manager on steroids.”
- **Key Details:**
  - Displays process hierarchy, open handles, loaded DLLs, CPU/memory usage, and verified signatures.
  - Highlights recently launched or suspicious processes in real time.
- **Use in Debugging:**
  - Identifies which process is locking a file or preventing an installer from running.
  - Checks for unsigned binaries or malicious software.

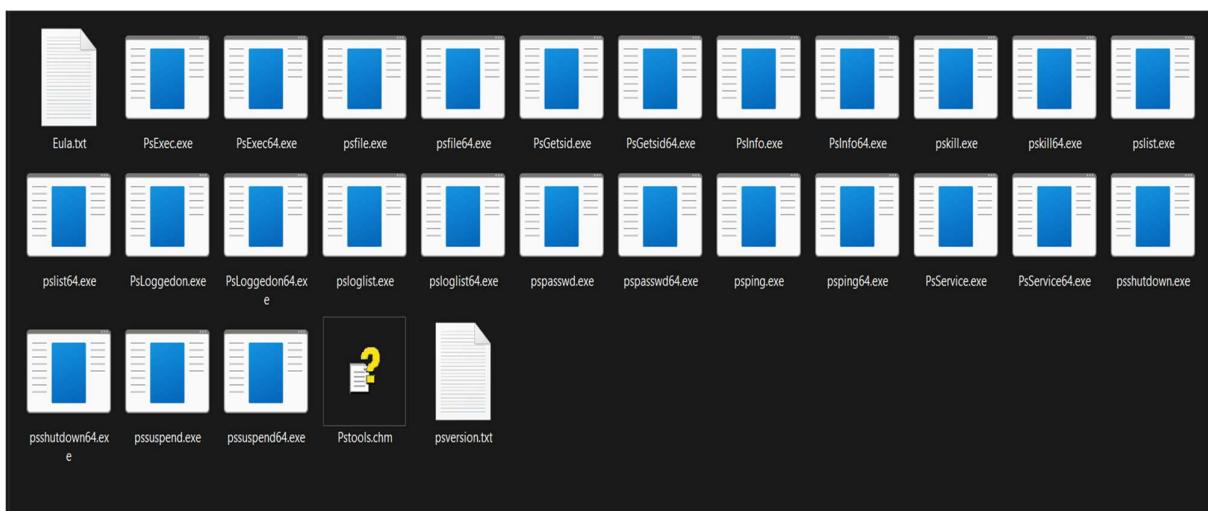


## 4. PsExec

- **Purpose:** Executes processes on remote systems or under different user contexts.
- **Key Details:**
  - Allows launching commands as SYSTEM, administrator, or another user.
  - Does not require manual login to the remote machine.
- **Use in Debugging:**
  - Testing MSI packages under SYSTEM context (similar to SCCM deployment).
  - Troubleshooting permission-related installation failures.

## 5. PsTools

- **Purpose:** A collection of command-line tools for remote administration.
- **Key Utilities in the Suite:**
  - **PsList:** View processes on remote systems.
  - **PsKill:** Terminate processes remotely.
  - **PsLoggedOn:** View logged-on users.
  - **PsShutdown:** Reboot or shut down systems remotely.
- **Use in Debugging:**
  - Manage processes and sessions across multiple machines in a testing lab.
  - Quickly restart services or kill problematic processes blocking an installation.



## 6. RegMon (Registry Monitor)

- **Purpose:** Monitors and logs real-time registry activity by applications and processes.
- **Key Details:**
  - Displays registry keys accessed, modified, or created by each process.
  - Supports filters for processes and paths to narrow down data.
- **Use in Debugging:**
  - Tracks registry changes during installation to understand application dependencies.
  - Identifies access denied errors causing setup failures.
- **Note:** RegMon is now merged into Process Monitor (ProcMon), which combines registry and file monitoring.

## 7. Whois

- **Purpose:** Looks up registration details of a domain.
- **Key Details:**
  - Provides information on domain ownership, registrar, and contact details.
  - Helps verify if a domain is legitimate.
- **Use in Debugging:**
  - Useful in security analysis when applications connect to suspicious external servers.
  - Validates network endpoints used by software.

Name	Date modified	Type	Size
Eula.txt	06-08-2025 12:14 PM	Text Document	8 KB
whois.exe	06-08-2025 12:14 PM	Application	390 KB
whois64.exe	06-08-2025 12:14 PM	Application	512 KB
whois64a.exe	06-08-2025 12:14 PM	Application	601 KB

## 8. Sysmon (System Monitor)

- **Purpose:** A Windows service and driver for logging detailed system activity into Event Viewer.
- **Key Details:**
  - Records process creation (with hashes, command line), network connections, and file creation events.
  - Supports custom configuration for filtering events of interest.
- **Use in Debugging:**
  - Tracks which processes and files are created by an installer or application.
  - Detects unexpected or malicious activity that standard event logs miss.

Name	Date modified	Type	Size
Eula.txt	06-08-2025 12:14 PM	Text Document	8 KB
Sysmon.exe	06-08-2025 12:14 PM	Application	8,282 KB
Sysmon64.exe	06-08-2025 12:14 PM	Application	4,457 KB
Sysmon64a.exe	06-08-2025 12:14 PM	Application	4,877 KB

## Conclusion

Each of these tools plays a vital role in application packaging, deployment, and security analysis. From monitoring process and registry activity (Process Explorer, RegMon, Sysmon) to managing remote executions (PsExec, PsTools) and session tracking (LogonSessions), they provide comprehensive visibility into Windows systems. Mastering these utilities helps in resolving installation issues, diagnosing application failures, and improving overall troubleshooting efficiency.

# Intune Free trial Subscription - How to enrol

## Step-by-Step: Enroll for Microsoft Intune Free Trial

### ◆ 1. Go to the Microsoft Intune Free Trial Page

- Open this link in your browser:

<https://www.microsoft.com/en-us/microsoft-intune>

- Click on "Try for free" or "Free trial" (you'll be redirected to Microsoft 365 trial).

The screenshot shows a Microsoft Learn page titled 'Try Microsoft Intune for free'. The URL in the address bar is 'https://www.microsoft.com/en-us/microsoft-intune'. The page content includes a note about Microsoft Intune helping to protect corporate data by managing devices and apps. It also lists prerequisites such as setting up a Microsoft Intune admin center and confirming MDM authority. A sidebar on the left provides navigation links for Microsoft Intune documentation, including 'Step 1 - Sign up for a free Intune trial' which is currently selected. The bottom of the screen shows a taskbar with various icons.

## ◆ 2. Sign in or Create an Account

- If you already have a Microsoft Work/School account, sign in.
- If not, create a new one during the process (e.g., admin@yourcompany.onmicrosoft.com).

**About you**   **Sign-in details**   **Complete & get started**

**Let's get you started**

Enter your work or school email address, we'll check if you need to create a new account for Microsoft Intune Plan 1 Trial.

Email

This is required

**Next**

**Microsoft Intune Plan 1 Trial**

**Signing up for your trial**

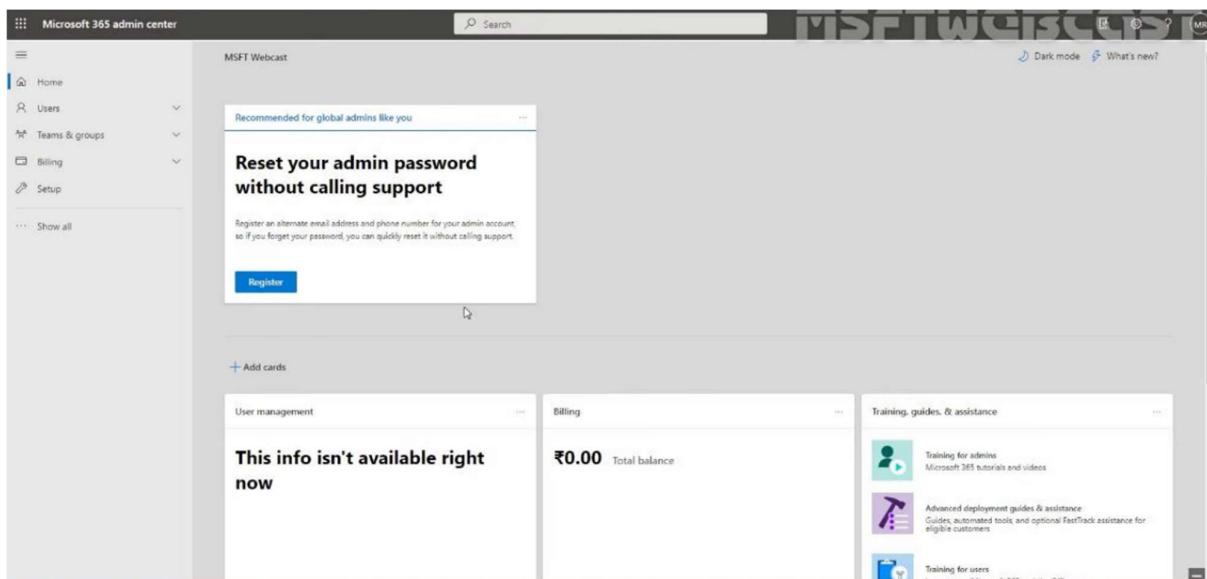
25 users allowed in 1-month free trial.  
Trial includes same features as the paid product.

**Product highlights**

- ✓ You must be a global, compliance, or billing admin. If you don't meet the role requirements, [contact Sales](#).
- ✓ Cut costs and complexity by managing any device with a single, unified tool already built into Microsoft 365. Gain full visibility into the health, compliance, and security status of your cloud and on-premises endpoints.
- ✓ Fortify your Zero Trust security architecture with a management solution that builds resiliency and centralizes endpoint security and identity-based device compliance. Help protect data on company-owned and bring-your-own devices.
- ✓ Empower IT to deliver the best possible endpoint experience through zero-touch deployment, flexible, non-intrusive mobile application management, and proactive recommendations based on Microsoft Cloud data.

### 3. 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.



### 4. 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.

## 5. 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.

